UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT SEATTLE.

UNITED STATES OF AMERICA,	
Plaintiff,	CASE NO. CR19-00159-RSL
v.	Seattle, Washington
PAIGE A. THOMPSON,	June 10, 2022 9:02 a.m.
Defendant.	JURY TRIAL, Vol. 4 of 9

VERBATIM REPORT OF PROCEEDINGS
BEFORE THE HONORABLE ROBERT S. LASNIK
UNITED STATES DISTRICT JUDGE

APPEARANCES:

For the Plaintiff:

ANDREW C. FRIEDMAN
JESSICA M. MANCA
TANIA M. CULBERTSON
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101

For the Defendant:

MOHAMMAD ALI HAMOUDI
NANCY TENNEY
Federal Public Defender's Office
1601 5th Avenue, Suite 700
Seattle, WA 90071

BRIAN E. KLEIN
MELISSA A. MEISTER
Waymaker LLP
515 S Flower Street, Suite 3500
Los Angeles, CA 90071

Reported by:

Nancy Bauer and Marci Chatelain
Official Federal Court Reporters
700 Stewart Street, Suite 17205
Seattle, WA 98101

INDEX

GOVERNMENT EXHIBITS

EXHIBIT	ADMITTED	WITHDRAWN
109-110	135	
112	116	
113	118	
114	132	
118-119	148	
122	192	
621	130	
720	11	
721	13	
750	28	
751	30	
752	31	
801	58	
850	189	
851	61	
852	64	
853	66	
854	68	
855	72	

DEFENSE EXHIBITS

EXHIBITS	ADMITTED	WITHDRAWN
1015	19	

PROCEEDINGS

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE CLERK: United States District Court for the Western District of Washington is now in session, the Honorable Robert S. Lasnik presiding.

THE COURT: Good morning. Thank you. Please be seated.

THE CLERK: We are resuming our jury trial in the matter of the United States versus Paige Thompson, cause number CR19-159, assigned to this Court.

THE COURT: And the government's next witness, please.

MR. FRIEDMAN: Your Honor, the government calls Matthew Pelaggi.

THE COURT: Okay.

Okay. Mr. Pelaggi, would you please come into the open area of the courtroom here, the well.

And please raise your right hand and my clerk will swear you in.

MATTHEW PELAGGI,
having been first duly sworn, testified as follows:

THE CLERK: If you could please state your first and last names, and spell your last name for the record.

THE COURT: And you can either keep the mask on or

take it off, whichever you prefer while you're testifying.

THE WITNESS: Okay. I'll probably keep it on.

THE COURT: Okay.

THE WITNESS: Hi. My name is Matthew Pelaggi. And my last name is P-e-l-a-g-g-i.

THE COURT: Go ahead, Mr. Friedman. Thank you.

MR. FRIEDMAN: Thank you, Your Honor.

DIRECT EXAMINATION

BY MR. FRIEDMAN:

Q. Good morning, Mr. Pelaggi.

A. Good morning.

Q. Where do you work?

A. I work for a company called Digital.ai.

Q. And has Digital.ai acquired other companies over the course of time?

A. Yes. Digital.ai acquired a company called Arxan.

Q. When did it acquire Arxan?

A. In 2020.

Q. And had Arxan itself acquired other companies before that?

A. It did back in 2017. It acquired a company called Apperian.

Q. And does Digital.ai still operate what was the Apperian business?

A. Digital.ai does, yes. It's now called Digital.ai App Management.

Q. And are you -- do you work on that business?
A. Yes. I'm the product owner for that product still.
Q. What is a product owner?
A. We prioritize futures from customers, resolve customer bugs, and work with the development teams to produce a better product.
Q. Okay. What business did you say that Apperian was in?
A. Apperian is a mobile application management company.
Q. Okay. So who -- what type of person would be an Apperian customer?
A. It's usually enterprise companies that want to distribute their applications -- their internal applications to their employees, and they don't want them to be listed in the public stores.
Q. So is this for companies that are not supplying computers or phones to their employees, the employees are bringing their own, kind of bring your own device?
A. Yeah, if it's a BYOD or bring your own device companies that are using this software.
Q. Okay. And what service does Apperian provide to those companies?
A. Apperian provides a portal that allows administrators to upload their applications there and apply different things to them.
And then we also provide a -- what we call an app catalog.

It's basically like the Apple App Store or Google Play store, but it's branded and internal only and delivers applications to their employees.

Q. Okay. So if I worked for IBM, if I worked for IBM, and if IBM were a customer of yours, I could go to this app store and download apps that would let me do whatever my job is?

A. Yeah. If you were at IBM, people would provide you a link to download the app store, and then you'd have access to all the internal applications that your company wanted you to have access to.

Q. And then does Apperian provide ongoing support and records of which employees have downloaded what versions of what app and help them use it?

A. Yes.

Q. Mr. Pelaggi, how long have you been at, let's say, Apperian and then its successors?

A. Since 2015.

Q. Are you aware of a breach that took place in 2019?

A. I am.

Q. Okay. And where does Apperian -- how does Apperian do its own computing? Does it have any relationship with AWS?

A. Yes. We have most of our services on AWS.

Q. Okay. What's your understanding of the breach?

A. My understanding is that on our servers we use products by a company called Apache, specifically something called Apache

httpd, which monitors like communications that go into the server and responds accordingly.

Q. Can I slow you down a moment?

A. Yes.

Q. Because, among other people in the room, there's a court reporter in front of you who has to take down what you and I say. And if you speak a little more slowly, it will make that easier.

A. Yes.

Q. Okay.

THE COURT: And if you spoke English instead of whatever you're saying, that would be nice, too.

Q. (By Mr. Friedman) Okay. So --

THE COURT: You used a lot of abbreviations. It would be great if you could just sort of slowly tell us what they mean.

THE WITNESS: Absolutely.

So Apache is basically an open-source company that provides software for different companies to use.

Q. (By Mr. Friedman) Okay. And so Apperian used Apache software?

A. Yes. We have web servers that host our data and things like this, and we used Apache products on that server.

Q. Okay. And there was a particular part of the Apache products that was involved in this?

A. Yes. So when we configured Apache on our servers, we used the default configuration recommended by them. And there's a module on there called mod_proxy.

Q. Okay. So let me slow you up again.

So what is a default configuration?

A. Just out of the box, like if you were to set up your phone, just like how it is set up by default without making any changes, is what we did with the modules we installed via Apache.

Q. Okay. Okay. And I cut you off.

A. No, that was it.

Q. All right. And so you -- the company used the default configuration for, what was this product?

A. It's called Apache httpd.

Q. Okay. And how did that relate to the breach?

A. It's my understanding that that specific module called mod_proxy was exploited in some way to gain access to our AWS system, and then retrieved credentials.

And once those credentials were retrieved --

Q. Can I stop you again? What do you mean by credentials?

A. It's basically user name and password or some other form of allowing our servers to verify that you're a user who has access.

Q. And then what happened once the credentials were retrieved?

A. Once the credentials were retrieved, data from our

databases were taken, as well as our source code and things like that.

Q. Okay. Did -- do you know how Apperian first learned that this had happened?

A. We -- one of our employees had just seen an article posted that showed a list of companies that were possibly impacted by a data breach and just the name Apperian was in the list.

Q. Okay. And once Apperian found out that there was a victim or possible victim of this, did it take any steps relating to mod_proxy?

A. Yes. We went back and removed mod_proxy from our configurations on our servers.

Q. Okay. And what did changing the configuration mean?

A. Just removing the mod_proxy module from the configuration.

Q. Did that take away the method of access that had been used?

A. Yes.

Q. Have you reviewed some data in this case?

A. I have.

Q. Okay. And was that data provided by the FBI to your company?

A. It was.

Q. What's your understanding of what the source was of that data?

A. The source of that data was basically taking information from our AWS account, so our database and our source code.

Q. Okay. And why were you reviewing this data?
A. I was reviewing this data because -- I was asked to.
Q. Fair enough.
What was your -- what were you supposed to do in reviewing it?
A. Verify that it was our information.
Q. Okay. Would you take a look at Exhibit 720?
MR. FRIEDMAN: And, Your Honor, this is one of the exhibits we offered yesterday, but I think it was deferred, so I think it's not yet in.
THE COURT: Okay.
Q. (By Mr. Friedman) Do you recognize that?
A. I do.
Q. Is that part of the material you reviewed?
A. It is part of the material I reviewed.
Q. That had been provided by the FBI?
A. Yes.
MR. FRIEDMAN: The government offers Exhibit 720.
MR. HAMOUDI: No objection, Your Honor.
THE COURT: 720 is admitted into evidence.
(Government Exhibit 720 admitted.)
Q. (By Mr. Friedman) So, Mr. Pelaggi, can you tell us what this is?
A. It's a list of different databases that belong to Apperian.
Q. Okay. And what did you conclude based on the fact that the

FBI had provided you this information?

A. That this is our data and that it had been taken.

Q. Did you look inside some of these -- is this a significant volume of data within these files or databases?

A. Yeah. It's a very significant volume of data, yes.

Q. Did you review a portion of the data?

A. I did.

Q. And based on what you reviewed, what did you -- what types of things did you see in the data?

A. I saw backups of our database. I was able to restore them and see our company -- or information about companies that use our products, their users, applications, things like that.

I was also able to find our source code and packages containing that code that are deployed on our production servers.

Q. Okay. Let me ask you about each of those.

You said your source code?

A. Yeah.

Q. What is source code?

A. It's just the -- it's basically what our product is. It's what the developers write. And then through writing that code, it's put in various places that allows customers to access our product.

Q. Okay. Did the data that you reviewed contain the complete source code for the product?

A. It did.
Q. Okay. Did it contain one or more copies of the complete database of information that you had?
A. It did.
Q. You talked a moment ago about restoring a file.
Would you look at Exhibit 721 and tell me if you recognize that?
A. I do.
Q. And I'm going to hope the next page is -- this page is relatively limited, but tell us what that is.
A. So on the left side, the backups.eu-central, that's a Amazon S3 bucket, which is basically just a place to store data and other information.
And then within that there is --
Q. Mr. Pelaggi, can I slow you up? Is this material you provided to the government after reviewing the data?
A. Yes.
MR. FRIEDMAN: Government offers Exhibit 721.
MR. HAMOUDI: I have no objection.
THE COURT: 721 is admitted into evidence.
(Government Exhibit 721 admitted.)
Q. (By Mr. Friedman) Okay. What's the first page of this exhibit?
A. So on the left side, the backups.eu, that is an Amazon S3 bucket, which is basically a place to store data and files like

that.

And then the next thing, the aire-db001, that is one of our database servers.

And then to the right of that is ease.dump, which is a complete dump of that database which contains all the information within it.

Q. And is -- that file highlighted in blue, the one you just referred to, is that the database that you tried to restore?

A. Yes.

Q. And how did you go about restoring that?

A. Basically, you can just Google how to restore a SQL database, which is just the type of database this is. And using free tools, you can do it on your local system.

Q. Did you succeed in restoring it?

A. I did.

Q. Could anyone who had gotten possession of this do that themselves and restore it?

A. They could.

Q. Would you look at the third page of this?

And do you recognize that?

A. I do.

Q. What is that?

A. That is the restored database and showing the schema, which is just basically a description of the database, and then different tables within it, like the accounts, analytics, and

applications tables.

And then underneath that, it shows the owners of those tables, identifying that it's an Apperian user who owns the tables, to me indicating that it is our product.

Q. And then were you able to go in and look at all of the underlying data in this database if you wanted?

A. Yeah, I was.

Q. Mr. Pelaggi, do you know whether the value of the data that was taken from Apperian was more than $5,000?

A. It's my understanding that it was.

Q. Okay. And why do you say that?

A. Because Apperian was acquired for much more than $5,000 back in 2017.

Q. Was it a several million dollars' purchase?

A. It was.

Q. And what was the value that was being bought when Arxan bought Apperian?

A. The Apperian product itself and its code base and employees who had worked with that product.

Q. Okay. And was all of that, basically -- if the entire code base was downloaded, was all of that in the information taken?

A. Yes.

Q. Would it cost more than $5,000 to reproduce the code to run a product like this?

A. Yes, it would.

Q. Did Ms. Thompson have any business relationship or employment relationship with Apperian?
A. Not that I'm aware of.
Q. Did Apperian intend for her to have access to its code and all of its data?
A. We did not.
Q. Did Apperian intend for her to have access to its computers?
A. No, we did not.
Q. Did Apperian intend for her to have access to any credentials to use those computers?
A. No, we did not.
Q. Did Apperian ever authorize her to use its computers or access them or take data?
A. No.

MR. FRIEDMAN: Thank you. I have no further questions.

THE COURT: Mr. Hamoudi will ask you some questions now on behalf of Ms. Thompson.

CROSS-EXAMINATION

BY MR. HAMOUDI:

Q. Good morning, Mr. Pelaggi.
A. Good morning.
Q. In March 2019, didn't Apache's website state that you should not enable your proxy until your server is secured?

A. I'm not aware of that statement.
Q. All right. And when you talk about Apache mod-sec, you're talk -- they provide a web access firewall; correct?
A. I can't speak to that.
Q. Okay. Were you involved at all with the investigation of the technology that was used in March 2019 with respect to this incident?
A. I wasn't involved in the investigation, no.
Q. Okay. And -- and so you don't have any personal knowledge of the technical processes that took place with respect to the information belonging to your company being downloaded to my client's computer; correct?
A. Can you repeat the question?
Q. Yeah.
You don't have personal direct knowledge of the technical processes that occurred for your data to be downloaded to my client's computer; correct?
A. Correct.
Q. Okay. I want to talk to you about a couple of things about data.
You looked through the data; correct?
A. Correct.
Q. Ms. Thompson didn't need to decrypt the data, did she?
A. Not that I'm aware of.
Q. Okay. And Ms. Thompson couldn't see the data until it was

downloaded; correct?
A. Correct.
Q. And you don't even know whether she viewed it; correct?
A. No, I don't.
Q. Okay. So I want to kind of walk you through the process that you went through looking at the data.
MR. HAMOUDI: Can we bring up defense marked next in order, Defense Exhibit 1015?
Q. (By Mr. Hamoudi) So you were provided a file by the United States Attorney's Office; correct?
A. Correct.
Q. And I put up on the screen an Excel spreadsheet. Do you recognize this spreadsheet?
A. I do.
Q. And this spreadsheet represents what?
A. Different servers in our systems and different backups of those -- the data on those servers.
Q. Okay. So let's go back to Exhibit, I believe it was, 720, which is previously admitted.
And so I'm going to walk you through this. The Excel spreadsheet that I just --
MR. HAMOUDI: I move to admit the Excel spreadsheet, Your Honor.
THE COURT: 1015, Defense Exhibit 1015 --
MR. FRIEDMAN: No objection, Your Honor.

THE COURT: -- is admitted into evidence.

(Defense Exhibit 1015 admitted.)

Q. (By Mr. Hamoudi) So walking the jury through this, and then if you look at the -- it says backups.us-east.gov.db.apperian. Is -- which of the files -- these are all your files, is that what you're talking about? These are the files on Ms. Thompson's computer?

A. So these are basically names of our servers. And then within those servers are backups of the data within them.

Q. Okay. So let's now go to the spreadsheet.

Okay. And are these the -- what do you call these lines? What would you call them in your experiences?

A. To me, this just looks like a different representation of the files that were shown in the previous exhibit with ease.dump at the end, so --

Q. These are the file paths; right?

A. Yes, file paths; correct.

Q. Okay, file paths.

And then let's go to the second page of 720.

Go to the second page, please.

Is there a second page?

Third page.

Go to 721.

All right. This helps. All right.

So this process showed that you looked into a file path,

backups.eu-central-1.db.apperian; correct?
A. Correct.
Q. And then you double clicked on that folder; correct?
A. Yes.
Q. And then you saw aire-db001.apperian.com; correct?
A. Correct.
Q. And then this file, ease.dump, is the file that you talked about that was of value to your company; correct?
A. Correct.
Q. All right. So now let's go back to the Excel spreadsheet.
Okay. This is the same file path; correct?
A. Correct.
Q. All right. So this is -- this is file path 11763; correct?
A. Correct.
Q. How many file paths were -- do you recall how many file paths there were that were in the files that were downloaded on Ms. Thompson's com- --
A. I really don't recall the specific number.
Q. Okay. Go to the bottom, the last part of this.
792,832; correct?
A. Correct.
Q. So out of the 792,832 file paths, within that file path, within three subfolders, was this database that is of value to your company; correct?
A. It's stored in other places, that was just the exhibit that

we selected.

Q. Okay. Did you happen to go through this entire file path?

A. No, I didn't.

Q. Okay. So you just sort of selectively went through particular file paths; correct?

A. Using things that I recognize with my experience working with the product, yes.

Q. Okay. So that's your experience with the product because you've worked with the company for several years; correct?

A. Yes.

Q. And when you talk about value, you talked about purchasing -- purchasing this code from the prior company. Would you have paid Ms. Thompson $4 million for this data?

A. As the owner of the product?

Q. Yeah.

Would the company have paid her $4 million if she showed up and said, I want $4 million for that? Would the company have paid her that?

A. I don't have any way to answer that because -- yeah, because that's outside of what I...

Q. Okay. Let me ask it a different way: Is it -- is this product worth any less or is this code worth any less because Ms. Thompson made a copy of it and downloaded it onto her computer?

A. It's -- I don't know if it impacts the value, but it

reveals things that we do and the fact that our product is unique and now somebody else could recreate this same product using this code and we wouldn't be able to do anything about that.

Q. Okay. So do you have any evidence -- does your company have any evidence that Ms. Thompson did that?

A. Not that I'm aware of.

MR. HAMOUDI: Okay. I have no further questions, Your Honor.

THE COURT: Okay. Thanks, Mr. Hamoudi.

Any redirect, Mr. Friedman?

MR. FRIEDMAN: One moment.

THE COURT: Sure. Take a moment.

(Off the record.)

MR. FRIEDMAN: No questions Your Honor.

THE COURT: You can step down. Thank you.

The government's next witness, Ms. Culbertson.

MS. CULBERTSON: The government calls Christopher Chan.

THE COURT: Okay.

Mr. Chan, would you please come forward into the open area here, the well of the courtroom.

And that's great, stand right about there and raise your right hand.

CHRISTOPHER CHAN,
having been first duly sworn, testified as follows:

THE COURT: Please have a seat up here.

THE CLERK: If you could please state your first and last names, and spell your last name for the record.

THE WITNESS: Sure. I'm Christopher Chan, C-h-a-n.

THE COURT: And, Mr. Chan, you can either leave your mask on or take it off while you testify, totally your call, okay.

THE WITNESS: All right. Thank you.

THE COURT: Okay. Go ahead, Ms. Culbertson.

DIRECT EXAMINATION

BY MS. CULBERTSON:

Q. Good morning, Mr. Chan.

A. Good morning.

Q. Where do you currently work?

A. I currently work at a company called Forcepoint.

Q. Okay. And what is your title there?

A. I am the VP of engineering for the SSE division.

Q. What does SSE stand for?

A. SSE stands for Secure Service Edge.

Q. In 2019, where were you working?

A. I was working at Bitglass.

Q. Bitglass.

And when was Bitglass founded?

A. Bitglass was founded in 2013.

Q. Was Bitglass eventually acquired by Forcepoint?
A. Yes.
Q. Okay. And when did that happen?
A. That happened October of 2021.
Q. Okay. So you formerly worked for a company known as Bitglass, it's now part of a company called Forcepoint?
A. That is correct.
Q. Okay. Just for clarity, ease of reference, I'm just going to refer to Bitglass for the rest of my questioning, if that's okay?
A. Yep.
Q. And where are you currently based?
A. Campbell, California.
Q. And what does or did Bitglass do? What kind of business is it?
A. We provided software for cloud security.
Q. Okay. And can you expand on that a little bit? What do you mean by cloud security?
A. So companies who have, you know, moved applications into the cloud, traditionally like email or storage or other applications into the cloud, we provide tools and applications to help them secure those applications with additional policies and procedures that allows them to be more compliant within their industry.
Q. Okay. And what does your particular job entail at

Bitglass?

A. I was the SVP of engineering and operations.

Q. Did you manage a team in that role?

A. Yes.

Q. And how many people did you manage?

A. About 50 people.

Q. Okay. And in your role, did you have knowledge of and experience with computer coding and computer scripts?

A. Yes.

Q. What kind of customers did Bitglass serve, what industries were the customers in?

A. Typically, you know, healthcare, finance, some retail, most of them that have compliance or security regulations that they have to comply by.

Q. And in 2019, about how many customers did Bitglass have?

A. I would say somewhere between 2 to 300.

Q. And did Bitglass use Amazon Web Services?

A. Yes.

Q. When did Bitglass start using AWS?

A. We started in 2013. When we built the company, we designed the application to be in the cloud to begin with and started using Amazon services starting then.

Q. Okay. So is it fair to say that you used AWS as part of your infrastructure?

A. That is correct.

Q. Okay. How did you first learn that Bitglass was involved in this case?
A. Our Amazon technical account manager contacted us, contacted me, and put us in touch with the Amazon security team.
Q. Okay. And about when was that?
A. That was November of 2019.
Q. Okay. So the technical account manager put you in touch with the AWS security team; is that correct?
A. That is correct.
Q. Okay. And then did the AWS security team put you in touch with anybody else?
A. Yes. He put us in contact with Special Agent Joel Martini.
Q. Okay. Is it your understanding he works for the FBI?
A. That is correct.
Q. Did you have a meeting with Special Agent Martini?
A. Yes.
Q. Okay. And was that meeting in person, over the phone?
A. It was over the phone or virtual.
Q. Okay. Did you agree to some follow-up actions at that meeting?
A. Yes.
Q. And what were those actions?
A. He provided information of a vulnerability that had occurred within our account and started providing us more information to investigate the issue.

Q. Okay. And did you agree to review some information that he was going to send you?
A. Yes.
Q. Okay. And did he actually send you that information?
A. Yes, he did.
Q. Okay. And did you look at it?
A. Yes. We looked at 'em.
Q. Okay. And what were you able to determine in looking at it as to who it belonged to?
A. That the information that was provided to us was an Amazon role that's associated with S3 resources that belong to Bitglass.

MS. CULBERTSON: Special Agent, can you pull up document 750, but don't publish it yet.

Q. (By Ms. Culbertson) Mr. Chan, you should be able to see on your screen shortly a document marked as Exhibit 750. Are you seeing it on your screen?

THE COURT: Not yet.

There we go.

Q. (By Ms. Culbertson) Do you recognize that?
A. Yes, I do.
Q. And what is it?
A. That is the list of S3 buckets that belong to Bitglass.
Q. And did Special Agent Martini send you this document?
A. Yes, he did.

MS. CULBERTSON: Your Honor, the government offers Exhibit 750.

MR. KLEIN: No objection, Your Honor.

THE COURT: 750 is admitted into evidence.

(Government Exhibit 750 admitted.)

Q. (By Ms. Culbertson) Okay. So at the top of this document, do you see s3_logrotate_role?

A. Yes, I do.

Q. And what is that?

A. That is the role, the name of the role, associated with our Amazon instance.

Q. Okay. And then what do you see underneath that? There's four entries.

A. Yes. Those are S3 buckets that, as the role name indicates, those are permissions for those four buckets that are shown.

Q. Okay. So the role -- if I'm understanding what you're saying, the role has permissions to access those four buckets?

A. That is correct.

Q. Okay. Do you recognize those as Bitglass buckets?

A. Yes, I do.

Q. Okay.

A. As you can see it has "bg" in it for Bitglass acronym.

Q. Okay. And who -- who at Bitglass was supposed to be able to use the s3_logrotate_role?

A. The logrotate role is really an internal operational role for data that is working with these buckets, only used specifically for rotating logs and storing them in S3.
Q. Okay. And can you explain to me what you mean by "log"?
A. A log is, first, operational logs, services that are -- servers that are logging their data to a local system that are rotated out into S3.
Q. Okay. Was the s3_logrotate_role intended to be used by the general public?
A. No.
Q. Okay.
MS. CULBERTSON: If you can call up, Special Agent, 751, but don't publish it yet.
Q. (By Ms. Culbertson) Okay. Mr. Chan, do you see a document in front of you marked as Exhibit 751?
A. Yes, I do.
Q. Okay. Do you recognize that document?
A. I do.
Q. What is it?
A. Those are one of our Apache server logs that come from one of the servers that had been put into that bucket.
Q. Okay. And is this a document that Special Agent Martini sent to you?
A. It is.
MS. CULBERTSON: Government moves to admit Exhibit

751.

MR. KLEIN: No objection, Your Honor.

THE COURT: All right. I'll admit 751, but it's going to make you dizzy.

(Government Exhibit 751 admitted.)

MS. CULBERTSON: We will try not to spend too long on this.

Q. (By Ms. Culbertson) Okay. So you said this was a Bitglass log file?

A. That is correct.

Q. So one of the S3 buckets that the logrotate_role could access?

A. Yes.

Q. And how do you recognize it as that?

A. The names of our servers are called prod-dataplane.

And this is one specific instance of it called prod-dataplane2.us-west2.

Q. Okay. And what does "prod" stand for in this context?

A. Prod stands for an environment, our production environment.

Q. Production environment? Okay.

MS. CULBERTSON: Special Agent, if you could call up 752, unpublished.

Q. (By Ms. Culbertson) Okay. Mr. Chan, do you recognize this document?

A. I do.

Q. Okay. Is this a document that Special Agent Martini gave you to review?
A. Yes, it is.
MS. CULBERTSON: Okay. The government moves to admit Exhibit 752.
MR. KLEIN: No objection, Your Honor.
THE COURT: 752 is admitted and can be displayed.
(Government Exhibit 752 admitted.)
Q. (By Ms. Culbertson) Okay. And, Mr. Chan, what is this document showing?
A. Again, logs from our operational service providing what we call data plane service, which is why we have the name dataplane, again, from prod-dataplane2.us-west2.
Q. Okay. And so this is a log that could be accessed using the role we've been talking about?
A. That is correct.
Q. Okay. So all of the documents we've just looked at given to you by Special Agent Martini contain Bitglass data or depict Bitglass data?
A. That is correct; that is Bitglass data.
Q. Was this data intended to be publicly available?
A. No, it was not.
Q. Who was supposed to be able to access this data?
A. Only authorized personnel from Bitglass are meant to actually use or see that data.

Q. How would a Bitglass employee go about accessing this data?
A. So our production network is obviously a private network. The only way to get into the network for any authorized personnel is first through a VPN access to the Bitglass corporate network from the VPN access which requires, obviously, account authorization and multifactor. They then have to access the environment through a jump -- we call it a jump box, so an access point into the production environment using SSH keys. So each individual will have an SSH key, along with a two-factor authentication through Google Authenticator.
Q. And can you tell me what an SSH key is briefly?
A. An SSH key is a combination of a public and private key where each user, authorized user, generates their own private key. And the public key is placed or authorized on the server to allow access to that environment.
Q. Did you try to figure out how this Bitglass data was taken out of your production environment or out of --
A. Yes. After connecting with both the Amazon security team, along with Special Agent Joel Martini, understanding the vulnerability that was in place on one of the servers, or through that role, through the Instance Metadata Service, which is only meant to be a local service, but because of the vulnerability, which was known to be a server-side request forgery, allowed that access to happen.
Q. As part of that investigation, were you able to determine

how much data was taken?
A. Yes.
Q. Was it a lot of data, a little data?
A. It was not a lot of data.
Q. Not a lot of data.
Was the data that was copied and taken important to Bitglass?
A. Important in the respect with respect to its operational data and it being private data, but it had no value externally other than internal operational use.
Q. So no external market value; is that fair to say?
A. Correct.
Q. Okay. So you talked a little bit about the vulnerability that allowed this to happen, that essentially a request -- is it fair to say that an external request was able to reach the Instance Metadata Service?
A. That is correct.
Q. And you said the Instance Metadata Service is intended to be private, it's not intended to be accessible externally?
A. That is correct.
Q. Okay. And are you aware how the Instance Metadata Service was contacted? Was it --
A. Yes.
Q. -- a particular technology?
A. Because the -- one of the features of our product, which is

a cloud security product, is a proxy, right. And so from a feature standpoint, our customers use our application, and where they would proxy their request through Bitglass so that policies and data retention and things like that can be enforced. And the instance or instances that the request went through for this vulnerability allowed a -- the proxied request to use that vulnerability and use the instance metadata interface unknowingly. That is not how it was meant to be done.

Q. Okay. Not how it was meant to be done.

So if I'm understanding what you said in layman's terms, essentially your product -- your application does allow for some Proxy Requests to pass?

A. That is correct.

Q. But it did not intend for Proxy Requests to pass to the Instance Metadata Service?

A. Correct; it was meant to be passed through the application so that policies could be enforced.

Q. Okay. And once you figured out this problem that external requests were being proxied to the Instance Metadata Service, did you fix it?

A. Yes, we did.

Q. What permissions -- turning back to the s3_logrotate_role that we've been talking about, what permissions were associated with that role specific to those S3 buckets we've been talking about?

A. Various ones, specifically S3, permissions like ListObjects, readObjects. There are some cases where you can actually write objects to the buckets.
Q. Okay. And can you tell me what a ListObject permission allows you to do?
A. List allows you to list the contents of a bucket.
Q. Okay. And I think you also said read?
A. Yes.
Q. What would a read --
A. Read would allow you to download the -- any object in the bucket to look at, obviously.
Q. Okay. As a cloud security company, was it important to Bitglass that it keep its data secure?
A. Absolutely. It's the number one thing, especially for a cloud security company.
Q. I'm sorry, can you say that again?
A. I said, "absolutely," that's the number one thing for a cloud security company is security.
Q. Okay. Are you aware whether the defendant in this case, Paige Thompson, had any professional association with Bitglass?
A. Not aware of any association.
Q. Did you intend for the defendant in this case to be able to access Bitglass's data?
A. No.
(Off the record.)

MS. CULBERTSON: Nothing further.

THE COURT: Mr. Klein, any questions for Mr. Chan?

MR. KLEIN: Yes, Your Honor.

THE COURT: Okay.

CROSS-EXAMINATION

BY MR. KLEIN:

Q. Good morning.

A. Good morning.

Q. I'm Brian Klein. I represent Ms. Thompson.

I'm going to start -- oh, I'm going to start off with a few questions here.

MR. KLEIN: Can you please pull up 751 and 752 for me? Can you please publish them?

Q. (By Mr. Klein) Do you see 751 and 752 in front of you, Mr. Chan?

A. Yes, I do.

Q. And those are the log files that the FBI provided you; correct?

A. Correct.

Q. Those log files are from 2015; right?

A. That is correct.

Q. And they're worth -- they're essentially worthless, aren't they?

A. Yes, they are.

Q. And you talked about how the FBI provided these to you and

told you that they came from Ms. Thompson's computer. Isn't it true that Ms. Thompson couldn't see this data until it was downloaded onto her computer, she could just see the titles of the -- the formatting titles?

A. That is correct.

Q. And you don't even know whether she ever viewed this data, do you?

A. I do not.

Q. And isn't it also true that Ms. Thompson didn't need to decrypt any of this data to view it, if she had viewed it?

A. That is correct.

Q. Now, you said -- you testified earlier that the only way to view this data -- and you -- excuse me, I'm going to paraphrase because it was long, but there was a VPN, a jump box, a multifactor authentication. Do you remember testifying to that?

A. Yes, I do.

Q. But that wasn't the only way, was it, because Ms. Thompson got this data; right?

A. It was not intended for users to see the data through that method.

Q. Okay. I'm not asking what was intended, I'm asking, was it the only way. There was actually two ways, wasn't there?

A. There was, yes.

Q. Now, are -- you talked about -- is it your conclusion that this was an SS -- sorry, I'll say this slower.

You discussed this being a server-side request forgery attack, didn't you, with the prosecutor?
A. It was not I who came up with that vulnerability terminology, it was brought to us through the Amazon security along with the FBI.
Q. Okay. So are you aware that Amazon has said publicly this was not a server-side request forgery?
A. I'm not aware of what they claim, other than my discussions with the people involved in this case.
Q. If they had said that publicly, would you dispute it?
A. I would not.
MR. KLEIN: One second, Your Honor.
THE COURT: Sure.
(Off the record.)
MR. KLEIN: Nothing further, Your Honor.
THE COURT: Anything else, Ms. Culbertson?
MS. CULBERTSON: No, Your Honor.
THE COURT: You know, Mr. Chan, I have a very skewed point of view on all this. I wonder, what does Bitglass mean? Why -- why do you call -- I mean, you know, they're words that are used by companies like Slack. If you were a slacker in my age, that's not a good thing; or square, we didn't like squares in the old days. What does Bitglass mean?
THE WITNESS: Well, the company was founded on the premise when we started back in 2013, and obviously the industry

was moving to the cloud, right, and companies who were providing security have traditionally been doing it within the enterprise, so they have applications, network devices, and things that they're protecting in the enterprise, but everyone's moving to the cloud. Their security challenges haven't changed, they're the same, and so we decided to build a company to solve that problem.

And where Bitglass came from was the idea that, you know, it was a glass into the data, a bit being, you know, computer data, so that we would put a glass and allow you to analyze the data. So that's the name Bitglass.

THE COURT: All right. Appreciate it. Thank you.

And, you know, the swag is great, too. I mean, I wanted to get some, you know, United States judge swag and the Marshals are like, no, you're not going to wear that in this climate, but maybe if I came up with gavel-git or something like that, we might be able to swing it.

Thanks very much. You're excused.

THE WITNESS: All right. Thank you.

THE COURT: Your next witness.

MR. FRIEDMAN: Your Honor, the government calls Vincent Kenney.

Oh, sorry.

THE COURT: Mr. Kenney, please come into the open area of the court here.

This way, yeah, it's a better -- it's kind of a tight squeeze there.

Great.

And if you'll please raise your right hand, my clerk will swear you in.

Right there's good.

Yeah.

VINCENT KENNEY,
having been first duly sworn, testified as follows:

THE COURT: Go ahead, Mr. Friedman.

MR. FRIEDMAN: Thank you, Your Honor.

DIRECT EXAMINATION

BY MR. FRIEDMAN:

Q. Good morning, Mr. Kenney.

A. Good morning.

Q. Where do you work?

A. I work for the Federal Bureau of Investigation.

Q. What do you do for the FBI?

A. I'm a computer scientist.

Q. Is that something you studied in school?

A. Yes. I majored in computer science.

Q. Okay. And what did you -- did you go right to work in computer science after that?

A. So right out of college, I worked as a software engineer for the Boeing Company.

Q. Okay. For how long did you do that?
A. I did that for two and a half years.
Q. And after that?
A. And after that, I was employed by the FBI, Salt Lake City Division, as a computer scientist.
Q. When did you start with the FBI?
A. I started in October of 2015.
Q. Okay. And are you assigned to any particular group that deals with virtual currency?
A. Yes. So in the Salt Lake City field office, I work on a cyber squad and work a lot of computer intrusions that involve cryptocurrencies and virtual currencies.
Q. Okay. And are you a member of more than just a group in that office?
A. Yes. I'm a member of a nationwide team in the FBI called the Virtual Currency Response Team, which is a team of experts in the FBI in the area of virtual currencies.
Q. As part of your work on that, do you analyze cryptocurrency transactions?
A. I do. I analyze cryptocurrency wallets, I analyze cryptocurrency transactions, and I provide training both internally in the FBI and externally to FBI partners.
Q. Mr. Kenney, let me start with a basic question: What's cryptocurrency?
A. Yeah. Simply, cryptocurrency is just a digital currency.

Q. Is there a -- what's the most well-known cryptocurrency?
A. So probably the most commonly used one and well-known one is Bitcoin.
Q. Has your work in this case related to a different cryptocurrency?
A. Yes, it has. It is related to the cryptocurrency Ether from the Ethereum network.
Q. And so let's use that as an example as you explain some of this to us.
A. Sure.
Q. Okay. You said cryptocurrency is digital currency?
A. It is, yes.
Q. What do you mean by that?
A. So digital currency is basically information that's stored in a record system that is passed from one person to another.
Q. If I want a physical coin or bill, can I get that?
A. No. It is not physical, it is information.
Q. Is it -- when I think of currency and maybe a $20 bill, that's backed by the U.S. government?
A. It is, yes.
Q. Is cryptocurrency backed by anyone?
A. It is backed by the participants of the network that use that cryptocurrency.
Q. So if someone has cryptocurrency and it's not tangible, where is that crypt- -- where does that exist or where is it

stored?
A. Yeah. So that is stored on a recordkeeping system called the blockchain.
Q. Are you familiar with a term called a wallet?
A. Yes, I am.
Q. What is a wallet?
A. A wallet basically stores the information that's needed for you to verify your ownership of a cryptocurrency.
Q. Okay. If a person wants to -- let's say, take someone who doesn't -- I don't have any cryptocurrency, and I want to get some Ether, what's the first thing I need to do?
A. Yeah. So all you would do is you would download wallet software to your computer or phone and you would set up a wallet and set up an address. And so from that address, you would then receive cryptocurrency to that address that you've set up.
Q. Okay. You said I'd set up a wallet?
A. Uh-huh.
Q. Where are wallets generally, at least?
A. Generally, wallets are stored on a computer.
Q. Okay. So likely to be stored on my computer?
A. Yes.
Q. And you mentioned an address. What is an address?
A. Yeah. So the address is a value that is stored on the blockchain that can have a certain number associated with it. And that number is the amount of cryptocurrency that is in that

address.
Q. Okay. Are you familiar with something called a public key?
A. Yes, I am.
Q. What's a public key?
A. So basically the way that you prove ownership is a public key is associated with that address. And so for you to prove you're the owner, you'll have a private key that will be paired with that public key. And therefore, that proves you are the owner of that public address.
Q. Okay. And what does proving I'm the owner of an address allow me to do?
A. It allows you to transact the cryptocurrency. So if you want to send that cryptocurrency amount to another address or someone else's wallet, you'll be able to prove you're the owner with that private key.
Q. What if I -- fair to say a private key is a very lengthy series of numbers and digits?
A. It is.
Q. Numbers and letters?
A. Correct.
Q. What if I lose my private key?
A. If you lose your private key, you can no longer prove that you're the owner of that cryptocurrency, and so therefore it cannot be moved.
Q. Okay. So I think you've told me how to get a wallet.

A. Uh-huh.
Q. Once you have a wallet, how do you get cryptocurrency?
A. Yeah. There are a few different manners. You can sign up for a cryptocurrency exchange and exchange U.S. dollars into cryptocurrency, or you can, you know, ask a friend who has cryptocurrency to send it to you.
Q. Okay. And then once I have cryptocurrency, what can I do with it?
A. You can then spend it on goods or services that accept that cryptocurrency.
Q. Okay. Are -- well, you're familiar with, what is the blockchain?
A. Yeah. So basically the blockchain is this recordkeeping system that is updated in a decentralized manner by participants on that network.
Q. Is there a -- in the physical world, is there a term that sort of you analogize to or use?
A. Yeah. So generally that updating process is what we call the mining process.
Q. All right. Let me slow you up for a moment.
A. Sure.
Q. Are you familiar with what a ledger is?
A. Yes, I am. So the blockchain is this recordkeeping system, and it acts as a ledger.
Q. Okay. And is there just one of it out there?

A. There is just one for that individual blockchain.
Q. Okay. Can people make copies of this ledger?
A. People can make copies of the ledger and create new cryptocurrencies with different ledgers.
Q. Is the ledger publicly available to anyone who wants to look at it?
A. It is. It is a public open system, and all the data that's stored in the system is publicly available.
Q. Okay. And I think you started to talk about how additional transactions are reflected in the ledger?
A. Correct.
Q. How does that happen?
A. So when additional transactions are appended to this ledger, there's a process that's involved to basically append new blocks to the blockchain, and that process is called cryptocurrency mining.
Q. And when you say a new block, what is a block?
A. A block is a segment of transactions that were made and appended to the ledger. So new transactions of someone trading cryptocurrency from one to another.
Q. Okay. What do you call people who perform cryptocurrency mining?
A. Yeah. So these are cryptocurrency miners.
Q. Okay. And how do they -- what does it mean to be a cryptocurrency miner?

A. Sure. Cryptocurrency miners are basically competing in a process, and that process is to solve an algorithm. And so when they solve the algorithm, the miner that solves it will add new transactions to the blockchain.

Q. Is an algorithm a fancy word for a math problem or maybe a complicated math problem?

A. It is.

Q. So these miners are racing to solve a math problem?

A. That's correct.

Q. And there's a reward -- well, what happens to the person who solves it first?

A. Yeah. So the person who solves the math problem is allowed to append new transactions to this recordkeeping system, and they receive a mining reward. And so that is built into the system for new cryptocurrency to be introduced into that network. And the miner who solves that problem receives that mining reward.

Q. So the mining reward is cryptocurrency?

A. It is.

Q. Okay. How much are you familiar generally with -- say you solve one of these problems, I don't know if you know in Bitcoin or Ether, but how often is there a problem to solve?

A. So the problem depends on the blockchain. For Bitcoin, it's about 10 minutes; for something like Ethereum, it's maybe about a minute.

Q. Okay. And how big a reward do you get for winning the contest and solving the problem?
A. So it depends as well. So for Bitcoin, it's about six and a half Bitcoin, for Ethereum, it's somewhere around that amount as well.
Q. Okay. Has there been a change in the nature of the problems and kind of the economics of the mining business?
A. Yeah. So when the blockchain and the cryptocurrencies first started, it's generally very, very easy to participate in this mining process. If you have a simple computer or a simple computing device, you can participate in that network as a cryptocurrency miner. As the network matures, this mining process becomes harder and harder and harder. And so as a result, today it is now more difficult to use a simple computing -- simple computer to actually mine cryptocurrencies.
Q. So what do people use -- what do you need to use today if you want to mine cryptocurrency?
A. Generally, what's helpful is using something like a graphics processing unit, or GPU, or also joining a mining pool, which is actually a collection of individuals who pool their computing resources together.
Q. And are they all necessarily in one place or they can be in multiple places?
A. They can be in multiple different places.
Q. So is it fair to say that a mining pool is a bunch of

people sharing computer resources in different locations trying to solve a math problem?

A. That's correct.

Q. Okay. If -- are there -- is there more than one mining pool out there?

A. There are multiple mining pools out there.

Q. Okay. If you're a member of the mining pool that wins one of these contests, what happens then?

A. So that mining pool receives the reward, and that reward is split up among participants of that mining pool.

Q. Okay. Are you familiar with -- a mining pool named Nanopool?

A. Yes, I am.

Q. Is that a well-known mining pool?

A. That's a commonly used one.

Q. If a person wants to start mining and being a member -- to be a member of Nanopool, how do they do that?

A. So they'll go ahead and sign up and download the Nanopool program. They'll get that set up on the computer they're going to use to mine cryptocurrency and start that process and join the Nanopool mining pool.

Q. What physical resources does a person need to successfully do that?

A. So someone just needs a computer, but, ideally, you need a computer with good computing power, such as graphics processing

units and other types of high-performance computing power.
Q. Okay. Is it expensive to mine cryptocurrency these days?
A. It is expensive. It's not only expensive to acquire that equipment, but it's also expensive to power that equipment with electricity.
Q. Is cryptocurrency mining less profitable than it used to be?
A. It is. Because of the difficulty of solving this math problem, it has become more of an optimization of both hardware and electricity to try and solve this problem in an efficient manner.
Q. Are you familiar with something called cryptojacking?
A. I am.
Q. What is cryptojacking?
A. Cryptojacking is compromising a computer and then putting mining software on that computer, and then using the resources from that computer to mine cryptocurrencies.
Q. When you say "compromising a computer," what do you mean by that?
A. I mean a computer intrusion, so intruding upon another person's computer without authorized access and then using the resources from that computer.
Q. Why would someone want to do that?
A. Because they don't want to pay for the resources that are involved in mining cryptocurrencies.

Q. And if you are cryptojacking, do you have any costs in electricity or computer equipment?
A. No. The victim, the individual who owns that computer and powers that computer, bears those expenses. You, as the individual doing the cryptojacking, just receive the mining rewards.
Q. Have you looked at some evidence -- electronic evidence in this case relating to accounts, electronic accounts, and posts by Ms. Thompson?
A. Yes, I have.
Q. Does that include Internet search history?
A. That does.
Q. In looking at that Internet search history, did you see searches relating to cryptocurrency mining or any of the other terms we've talked about?
A. Yes.
Q. Okay. And I'm going to ask you to look at Exhibit 504, the second page.

(Off the record.)

MR. FRIEDMAN: Sorry, Your Honor, this is in a different format.

(Off the record.)

Q. (By Mr. Friedman) When you looked at the Internet search history, what types of reference did you see to cryptocurrency mining?

A. I saw various different searches for crypto -- general cryptocurrency mining information.
Q. Did you see searches relating to a particular type of cryptocurrency?
A. Yes; Ethereum and Ether.
Q. And did you see searches relating to a particular mining pool?
A. Yes; Nanopool.
Q. Let me ask you, have you seen -- I'm going to show you a Twitter message. This is Exhibit 436. It's actually a conversation.
A. Okay.
Q. Is this a record that you've seen before?
A. Yes.
Q. And this is admitted.
A. Yes, it is.
Q. Is it fair to say, Mr. Kenney, this is a conversation between two people --
A. Yes, it is.
Q. -- with five statements or -- do we read from top to bottom or bottom to top?
A. Bottom to top.
Q. And is it fair to say the message is a message sent to Ms. Thompson's account?
A. Yes, it is.

Q. What was that message?
A. How are you supporting yourself.
Q. What was Ms. Thompson's response?
A. Just living with friend and hacking EC2 instances and getting access to some AWS accounts and using them to mine crypto.
Q. And did that prompt another question to Ms. Thompson?
A. Gotcha, what are you mining?
MR. KLEIN: Objection, Your Honor, the document speaks for itself.
THE COURT: Yeah, but I'll allow it.
Go ahead.
Gotcha, what are you mining.
Q. (By Mr. Friedman) And then a follow-up question?
A. ETH.
Q. What do you understand ETH to mean?
A. ETH is the symbol for Ether.
Q. And then did Ms. Thompson respond to that?
A. ETH/Monero.
Q. What is Monero?
A. Monero is another type of cryptocurrency.
Q. Okay. Would you take a look at Exhibit 462, page 4? This is an Internet Relay Chat message that's already been admitted.
And could you read the first of the three statements here?
MR. KLEIN: Objection, Your Honor. Foundation.

MR. FRIEDMAN: Your Honor, I believe this document was admitted yesterday.

THE COURT: I don't understand the objection. It's admitted into evidence.

MR. KLEIN: Yes, but what's his foundation to know about this document, Your Honor, that's what I'm objecting to.

THE COURT: Okay. Go ahead, do that.

Q. (By Mr. Friedman) Did you read this investigation as part of reviewing Ms. Thompson's social media posts?

A. Yes, I did.

Q. And do you have an understanding about one of the terms I'm about to ask you what that means in plain English?

A. Yes.

THE COURT: Okay, that's good enough.

MR. FRIEDMAN: Thank you, Your Honor.

THE COURT: Objection is overruled.

Q. (By Mr. Friedman) Would you just read out loud the first of the three messages here?

A. Sure. The one is, like I've straight up gone to my counselor, told her that I was hacking stuff and stealing CPU time to mine crypto and buy new things for myself and wear new designer clothes, et cetera.

Q. There's a reference here to stealing CPU time. What does that mean?

A. That means stealing computing power and computing

resources.
Q. Does CPU stand for something specific?
A. Yes. CPU stands for central processing unit.
Q. Okay. And is that a reference to part of a computer or part of a computer's function?
A. Yes.
Q. Can you tell us what that part is?
A. Yeah. That is basically the processor that powers calculations for that computer.
Q. And would you take a look at a text, Exhibit 502? This is a text message sent by Ms. Thompson. I'm going to ask you just about the two green messages here.
A. Okay.
Q. Would you read the first message?
A. I have about 5,000 a month coming in now, but it's all in Ethereum, and I have to find a safe way to convert.
Q. Do you have an understanding of what a safe way -- what a way to convert refers to?
A. Yes. That could be receiving Ethereum tokens and wanting to exchange that into U.S. dollars or some other type of format to spend them.
Q. And why would a person want to exchange Ethereum for dollars?
A. Maybe the items they want to buy, they can't use to purchase those with Ethereum, so they'll need to exchange it

into a currency that they can use to purchase those items.
Q. Okay. And would you read the second message here?
A. Because I'm hacking AWS accounts, I get to use EC2 GPU miners.
Q. I think you added an extra I as you read it.
A. Oh, I get it using EC2 GPU miners.
Q. Okay. What is an ECU -- or let me ask you more centrally, what does GPU refer to?
A. Yeah. So GPU is the graphics processing unit.
Q. Okay. And what is a graphic processing unit?
A. So a graphics processing unit is similar to a CPU, but it's actually a much faster processing unit, so it can do even more intense calculations.
Q. Okay. And why would you want to use that kind of unit to mine cryptocurrency?
A. Because that's actually a more efficient chip to actually mine cryptocurrency.
MR. FRIEDMAN: Okay. And if we could turn to the second page of this exhibit.
Could we focus on the third text down?
Q. (By Mr. Friedman) Would you read that?
A. One way is to start buying drugs, gift cards, et cetera, and stealing them too.
Q. I think you misread a word.
A. And selling them, sorry, selling them to convert back into

currency.
Q. Okay. And does this refer to the issue of converting to currency that you were talking about a moment ago?
A. Yes.
Q. What is the reference to gift cards? Do you understand what that would be in this context?
A. Yeah. So I guess if someone wanted to buy gift cards with cryptocurrency, that could be one way to convert the cryptocurrency to a form of payment that they can use.
Q. Would you take a look at Exhibit 801?
This has not yet been admitted.
Do you recognize this?
A. Yes, I do.
Q. What's your understanding of what this is? Not the details of it, where it came from.
A. Yeah. So this was a script that Waymon received from the subject's computer.
Q. When you say "Waymon," to whom are you referring to?
A. Waymon Ho, computer scientist out of the Seattle field office.
MR. FRIEDMAN: Your Honor, the government intends to offer this through Mr. Ho, and so we do it provisionally now, unless there's no objection.
MR. KLEIN: We don't object, Your Honor.
THE COURT: Okay. 801 can be admitted now subject to

Mr. Ho seeing it.

(Government Exhibit 801 admitted.)

THE COURT: And you can display it.

MR. FRIEDMAN: Thank you, Your Honor.

Q. (By Mr. Friedman) Okay. You said your understanding is this was something that was on Ms. Thompson's computer?

A. Correct.

Q. Okay. What, in general -- let's start at the very bottom of this. What is the bottom two or three lines -- two lines?

A. Yeah. So the very bottom line that starts /ethminer, that is a program that was run to join the Nanopool mining pool and participate as a miner.

Q. Okay. And although this script was found on the computer --

A. Uh-huh.

Q. -- you don't know what computer that program was run on or where that software was installed, do you?

A. Correct.

Q. Okay. But this would be an instruction for some computer to join Nanopool?

A. Correct.

Q. And then at the top, do you see additional information relevant to joining Nanopool?

A. Yeah. So at the very top, a few lines down where it says "export ETH_ACCT," that is the address that will receive funds

from participating in the mining pool.
Q. ETH_ACCT, what does that mean?
A. That would be Ethereum account.
Q. Okay. So this is for mining Ethereum?
A. Correct.
Q. And then are all those digits after that the address?
A. That is the address.
Q. Okay. Because it's hard to remember those, I'm going to refer to them just by the first six digits, perhaps the --
A. Sure.
Q. -- 0x5a86?
A. Correct.
Q. Okay. Is that the only address that you're aware of in this case that starts with those six figures?
A. Yes.
Q. Did you do some analysis relating to that wallet?
A. I did.
Q. Okay. And tell us in general terms, how did you start doing that analysis?
A. Yeah. So I started by going to an online block explorer and entering that address, that account, into the online block explorer.
Q. What is a block explorer?
A. So a block explorer is an easy way to view these records that are kept on the blockchain.

Q. Okay. And you said you went to one called Etherscan?
A. Correct.
Q. Is that a well-known block explorer?
A. That is a well-known one.
Q. In your experience, has the information that you found on there generally been accurate and reliable?
A. Yes.
Q. How do you know that or what did you check that against?
A. So I can verify that by downloading the full Ethereum blockchain and confirming that information with a local copy of Ethereum blockchain.
Q. And as we walk through your analysis, is that something you ultimately did in this case?
A. It is.
Q. Let's first talk about what you found with the block explorer.

Would you look at Exhibit 851 and tell me if you recognize that?

A. Yes, I do.
Q. What is that?
A. That is the main page for the address that we saw in the prior document.

MR. FRIEDMAN: The government offers Exhibit 851.

MR. KLEIN: No objection, Your Honor.

THE COURT: 851 is admitted.

(Government Exhibit 851 admitted.)

Q. (By Mr. Friedman) So, in general terms, what does this page show?

A. This page shows different transactions that were made to that particular address.

Q. Okay. Is it a -- it's a list of transactions?

A. It is a list.

Q. And is it all of the transactions to the wallet or are we just looking at one page?

A. We're just looking at a partial amount of the transactions.

MR. FRIEDMAN: Okay. And Special Agent Martini is just blowing that up.

Q. (By Mr. Friedman) For what period were you looking at transactions?

A. Yes. I was looking from March 10th to August 15th -- I'm sorry, August 5th, 2019.

Q. Okay. But were you looking more broadly, even if that's what you found?

A. I looked at the total sum of transactions.

Q. Let me stop you.

Were you looking more broadly in 2019 to see if there were other transactions, but that -- these are the ones that you found?

A. Correct.

Q. Did you look for the entire year of 2019?

A. I did.
Q. Okay. And were you looking for just incoming or incoming and outgoing?
A. I was primarily looking for incoming, received transactions.
Q. Okay. So these are incoming transactions during that period?
A. Correct.
Q. Okay. And now, can you tell me, what was -- what transactions did you find? What was the beginning and the end, first and last?
A. Sure. So in this list, you can see that a number of these transactions or all of these, really, were coming from a recipient called Nanopool to a particular address of interest.
Q. Right, but what was the time period? What was the first transaction that you found?
A. Ah, it was March 10th.
Q. And what was the last incoming transaction that you found?
A. August 5th.
Q. And in total, how many incoming transactions did you find for 2019?
A. 261.
Q. Okay. And is it fair to say that each line on the screen that we're looking at now is one transaction?
A. That's correct.

Q. So what information were you able to pull about each of those transactions?
A. Yeah. So I was able to pull the transaction hash, which is the unique value associated with it, the block number, so what block it was appended to in the blockchain, and then the from and the to recipient of that transaction, and then also the amount that was received.
Q. And the date and time in the central column?
A. And the date and time, yes.
Q. Okay. Of the 261 transactions that you found, from whom did those come?
A. Those came from a recipient named Nanopool.
Q. Okay. So all of them were Nanopool?
A. Correct.
Q. And this probably is going to be not surprising, you were searching for one wallet; correct?
A. That's correct.
Q. Was the recipient of all the 261 then the owner of that wallet?
A. Correct.
Q. And where do you see that here?
A. So I can see that here under the "to" address.
Q. Okay. Each of those starts with a 0x5a86?
A. Correct.
Q. Okay. Once you had done this and identified the 261

transactions, what did you do next?
A. I then looked at an individual transaction hash for this particular transaction or for all transactions.
Q. Okay. Is exhibit -- take a look at Exhibit 852 and tell me if that reflects that.
A. Yes. This is the transaction details from a specific transaction hash.
MR. FRIEDMAN: Government offers Exhibit 852.
MR. KLEIN: No objection, Your Honor.
THE COURT: 852 is admitted.
(Government Exhibit 852 admitted.)
Q. (By Mr. Friedman) Okay. And so the first line here is transaction hash?
A. Correct.
Q. Is that the code number or identifier for this particular transaction?
A. That's the unique identify for this particular transaction.
Q. And what information were you able to derive about this transaction?
A. Yeah. I could derive that it comes from block 7460822, and that it was made on March 29th, 2019. And in particular, in this display, I can see the address that's associated with Nanopool, the "from" address and then the "to" address, which is the address we saw in that script previously, 0x5a86.
Q. Okay. And do you see the value of this particular

transaction?
A. I also do see the value.
Q. About a fifth of an Ether?
A. Correct.
Q. Okay. At this point, was this the end of your analysis using the block scanner, and did you switch to looking at something else?
A. Yes. So this is where I concluded using Etherscan. And then from here, I moved to confirm this information with a local archive node of the Ethereum network that I've downloaded and set up in an offline environment -- or in a stand-alone environment, rather.
Q. You downloaded the entire Ethereum blockchain?
A. Correct.
Q. And that's what you're referring to as a node?
A. Correct.
Q. Okay. Did you look at the node for each of the 261 transactions?
A. I did. So by standing up a local node, I was able to programatically make these requests for all 261 transactions.
Q. Okay. Does Exhibit 853 show part of that process?
A. Yes. This is the local explorer that I have setting up on the machine that shows the individual block, that 7460822 block, in the local archive node that I have.
MR. FRIEDMAN: Okay. Government offers Exhibit 853.

MR. KLEIN: No objection, Your Honor.

THE COURT: 853?

MR. FRIEDMAN: Yes, Your Honor.

THE COURT: Is admitted.

(Government Exhibit 853 admitted.)

Q. (By Mr. Friedman) So, Mr. Kenney, this is a record relating to one block; right?

A. Correct.

Q. But it's a block that had a transaction in which you were interested?

A. Correct.

Q. And so did you do this 261 times, I guess, unless some blocks overlapped?

A. Correct.

Q. Okay. What information did you get by doing this about this particular transaction?

A. So what I can tell is that the block has a block number, it has some other information pertaining to the cryptocurrency mining, but, in particular, it has the miner that mined and appended this block to the blockchain, identified as 0x52bc. And in particular, when the miner appends this block to the blockchain, they will append their organization and their name. And so what I can see in the data translated that this was appended by Nanopool.org.

Q. The fact that Nanopool is appending it means Nanopool won

this competition; right?
A. That's correct.
Q. And Nanopool received a reward?
A. That's correct.
Q. And that's why Nanopool is paying its members?
A. Correct. The reward was sent to that 0x52bc miner address.
Q. Okay.
THE COURT: I see the phrase gas limit and gas price, what does that refer to?
THE WITNESS: These refer to transaction fees that are involved in powering the network.
THE COURT: Why do they call them gas?
THE WITNESS: Because Ethereum allows you to do multiple different computing functions, and so they refer to that as gas or power to be able to do these multiple computing functions.
THE COURT: Okay. Thank you.
THE WITNESS: Sure.
Q. (By Mr. Friedman) Mr. Kenney, after you had done this 261 times, or perhaps a couple less, I'm not sure, did you prepare a spreadsheet that summarized -- that took all of the data you had received and put it into one spreadsheet?
A. Yes.
Q. Would you look at Exhibit 855, which should be a spreadsheet in native format.

(Off the record.)

MR. FRIEDMAN: Your Honor, I neglected to offer 854, so I'd offer that.

THE COURT: That's the one we just saw.

MR. FRIEDMAN: We just saw it. My co-counsel told me I forgot to offer it and that maybe just we were seeing it?

THE COURT: Did we admit 854, Victoria?

THE CLERK: We haven't seen it.

MR. FRIEDMAN: We haven't. I'm sorry.

They're actually telling me I skipped a line and didn't show 854.

Could we look at Exhibit 854 first?

THE COURT: Sure.

Q. (By Mr. Friedman) Okay. Do you see Exhibit 854?

A. I do, yes.

Q. Is this the next -- the next-to-last step in your analysis?

A. This is. So this is --

MR. FRIEDMAN: Can I offer it first?

Government offers Exhibit 854.

MR. KLEIN: One sec, Your Honor, I'm just going to look at it real quick.

THE COURT: Sure.

MR. KLEIN: No objection.

THE COURT: 854 is admitted.

(Government Exhibit 854 admitted.)

Q. (By Mr. Friedman) Tell us what this reflects.
A. Okay. So this is me entering in a single transaction that I observed. And from that transaction, I can see the unique transaction value just under the big word Transaction. And from there, I can see two addresses listed under that transaction value. The same address that I saw in the previous slide, 0x52bc that we associated now with Nanopool, and that's being sent to our address of interest from the script that we were looking at at the beginning here, 0x5a86. And the received amount into that address was 0.2061 ETH.
Q. Okay. And so this is just looking inside the block on the last slide and pulling the transaction out for more detail?
A. Correct. And this is the process that I used to pull out all 261 transactions that were associated with that address.
Q. That you put into your spreadsheet?
A. That I put into the spreadsheet.
Q. Great.
Let's look at Exhibit 855.
Is this the spreadsheet that you created?
A. Yes.
MR. FRIEDMAN: The government offers Exhibit 855.
MR. KLEIN: Your Honor, we don't have a hard copy of that. I'm not saying I am going to object, but I would like to look at -- since it's a whole spreadsheet, to somehow have a chance to review it.

(Off the record.)

THE COURT: Should we take a break now, then you can look at it during the break?

MR. KLEIN: I would appreciate that, Your Honor.

THE COURT: So we'll take our midmorning break and start up again at -- how about everybody be back at 20 of, okay? We'll go a little bit longer for the break.

And head on down to Judge Pechman's courtroom.

Thank you, Victoria.

Please stay in your seats until the jury has a chance to travel.

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: Okay. You can step down, Agent. Thank you.

We'll start up again at 20 of, everyone in their chairs then. Thanks.

MR. FRIEDMAN: Your Honor?

THE COURT: Yes.

MR. FRIEDMAN: There's probably a couple minute -- a couple housekeeping and scheduling issues we'd like to raise with the Court. I don't know if the Court -- if the Court has -- if we could do that at the start of the lunch break or the end of the lunch break, if the Court has a few minutes.

THE COURT: Let's do it at a little bit before noon,

is that okay?

MR. FRIEDMAN: That's fine.

THE COURT: Good.

MR. FRIEDMAN: Thank you.

THE COURT: Let them know what you're going to talk about so they're not blindsided.

MR. FRIEDMAN: Sounds good. Yep.

THE COURT: Yeah.

MR. FRIEDMAN: I don't think they will be.

THE COURT: Okay.

You're a little bit ahead of schedule; right?

MR. FRIEDMAN: The next witness is the -- will be --

THE COURT: The long one, I understand.

MR. FRIEDMAN: Yeah.

I think we're, I'm going to guess, within -- you know, within an hour of schedule. It's like the closest I've ever been.

THE COURT: But you're not anticipating going into anything more than maybe Wednesday morning or something like that?

MR. FRIEDMAN: I think we would rest Tuesday, would be my guess now.

THE COURT: Tuesday, probably. Okay.

MR. FRIEDMAN: Yeah.

THE COURT: And my intention is to give you a proposed

set of jury instructions today for you to look at over the weekend, too, so...

MR. FRIEDMAN: Thank you, Your Honor.

THE COURT: Did you want to say anything, Mr. Klein?

MR. KLEIN: No.

THE COURT: Okay. Great.

We're adjourned.

(Court in recess 10:21 a.m. 10:42 a.m.)

THE FOLLOWING PROCEEDINGS WERE HELD
IN THE PRESENCE OF THE JURY:

THE COURT: Mr. Klein, did you do what you wanted to do?

MR. KLEIN: Yes, Your Honor. We're not going to be objecting.

THE COURT: No objection to the exhibit. It's admitted, whichever one it was.

MR. FRIEDMAN: 855.

THE COURT: 855. Thank you.

(Government Exhibit 855 admitted.)

THE COURT: You can continue, Mr. Friedman.

MR. FRIEDMAN: I have to wait for it to get called up. There we go. Thank you.

Q. (By Mr. Friedman) So Exhibit 855 is the spreadsheet that you prepared summarizing your results from the 261 searches?

A. That's correct.

Q. And we're looking at the top-left corner of that now?
A. Correct.
Q. In each line of this spreadsheet, does that have data that reflects one of those 261 searches?
A. That's correct. These are different fields from that specific transaction.
Q. Okay. And rather than ask the special agent to scroll down, is it fair to say this is 261 lines long?
A. Correct.
Q. If we could go to Columns P, Q, and R. What does that part of the spreadsheet reflect?
A. So P reflects the price of Ethereum, or Ether, one Ether, at the time when this transaction was made.
Q. Can I stop you for a moment?
A. Yes.
Q. Are these transactions roughly one per day --
A. One single --
Q. -- one line per day, roughly?
A. Roughly, yes.
Q. So an Ether was worth $142 on the first day?
A. Correct.
Q. $177 the next day?
A. Yes.
Q. Then it plummets to $138?
A. That's correct.

Q. Back to $240 the next day?
A. Correct.
Q. Why is it changing that much and that fast?
A. Yeah. So what gives these things value is their tradability and the price people will accept for the traded token. So as a result, the price will fluctuate in the value of these particular cryptocurrencies.
Q. A lot and quickly?
A. It can be, yes.
Q. So that first column is the daily price for Ether?
A. Correct.
Q. What is the second column?
A. That is the value that was received in this transaction.
Q. So for first transaction, a fifth of an Ether?
A. Correct.
Q. And what is the third column?
A. That is the amount of that value in U.S. dollars.
Q. So you basically said a fifth of $142 was about 30 bucks?
A. Correct.
Q. And then did you total the amount of Ether received and the dollar value?
A. I did.
Q. Is that at the bottom of the spreadsheet?
A. It is.
MR. FRIEDMAN: Can you scroll down, Agent?

Q. (By Mr. Friedman) And what totals did you come up with?
A. The total amount in Ether is 55.2773841, and that is $10,014.03.
Q. All to this wallet?
A. Correct.
Q. Were there a couple other wallets you saw in the case?
A. A value sent to those couple other wallets?
Q. Not that you searched, but are you aware of other wallets that were -- of which evidence was found on Ms. Thompson's computer?
A. There were other wallets, but, in particular, in this spreadsheet, I was looking at this --
Q. You analyzed so this is for this one wallet?
A. Yes.

MR. FRIEDMAN: Thank you very much, Mr. Kenney.

THE WITNESS: For sure.

THE COURT: Mr. Klein, questions for Mr. Kenney?

MR. KLEIN: Yes, Your Honor.

CROSS-EXAMINATION

BY MR. KLEIN:

Q. Good morning. I'm Brian Klein. I represent Ms. Thompson.
A. Good morning.
Q. When did you start working on this case?
A. I started working on this case roughly around March of 2022.

Q. And who have you spoken with at the FBI about this case?
A. I've spoken with Special Agent Joel and Computer Scientist Waymon Ho.
Q. Have you spoken with the prosecutors?
A. I spoke with the prosecutors for the past few weeks, yes.
Q. And was that about preparing you for this testimony?
A. Correct.
Q. Did you ever speak to anyone else about this case, outside of the FBI and the prosecution team?
A. No.
Q. Never spoke to any of the companies?
A. No.
Q. I'm going to start off talking about Ethereum or ETH. So Ethereum is the blockchain, right?
A. Correct.
Q. And then the digital currency that goes on it -- the cryptocurrency is ETH?
A. Correct.
Q. And it's legal to own ETH?
A. It is legal to own it.
Q. It's legal to transfer it?
A. It is legal to transfer it.
Q. And it's legal to mine it?
A. On your own equipment, it's legal to mine it.
Q. Setting aside your testimony about cryptojacking, it's

legal to mine?
A. The process of mining is legal.
Q. Yes.
And then you talked about Nanopool. What do you know about Nanopool?
A. Nanopool is basically a pool that you can join to mine cryptocurrencies.
Q. Do you know where it's located?
A. I don't know where it's physically located because it's a decentralized and distributed mining pool.
Q. It is a public web address, right, nanopool.org?
A. Yes.
Q. And it's, actually, owned by a German family, correct?
A. Okay.
THE COURT: When you say "okay" -- if you don't know, just say, "I don't know," because --
THE WITNESS: Okay.
THE COURT: -- what he says is not evidence --
THE WITNESS: Okay.
THE COURT: -- it is just a question. So I don't want any confusion.
THE WITNESS: Okay. I'm aware of that now.
MR. KLEIN: Should I ask the question again, Your Honor?
THE COURT: No, don't ask it, because it's about

German. Ask another question.

Q. (By Mr. Klein) But participating in Nanopool, people all over the world participate in Nanopool?

A. They do.

Q. People in the United States?

A. People in the United States.

Q. As far as you know, it's perfectly legal?

A. It is legal as long as you're using your own equipment.

Q. With that caveat?

A. Correct.

Q. Let's talk for a moment about private keys. So can you explain what a private key is again?

A. Yeah. Basically, a private key is a series of numbers and letters that proves you're the owner of a particular cryptocurrency address.

Q. Okay. And that's true for Bitcoin?

A. Yes.

Q. It's also true for Ether?

A. Yes.

Q. Okay. And that address, is that the public address? Is that the public key?

A. So the public key is a slightly different key that's used to pair with the private key. The address that you see on the blockchain is the one that's associated with your amounts.

Q. Okay. And unless someone identifies that address as

themselves, you don't know who controls that address; is that right?

A. That's correct. Addresses are pseudoanonymous.

Q. And by that, you mean -- what did you mean by that?

A. Yeah. I mean that the addresses exist on the blockchain, but in the special letters and numbers format. There isn't someone's name associated with that address.

Q. But I'm talking about Ether right now, just to be very clear.

A. Correct.

Q. Okay. And so one person could have a private key, right?

A. Correct.

Q. Multiple people can have a private key, also, correct?

A. Correct.

Q. Hundreds of people can have the same private key, correct?

A. Well, if hundreds of people had the same private key to that particular address, then those hundreds of people could prove they're the owner of that address.

Q. But hundreds of people could have the same private key?

A. They feasibly could.

Q. Okay. Let's talk about wallets for a second. What is a wallet, again?

A. A wallet is basically a program that's a container for private keys. So you'll set up a wallet to keep and contain your private keys.

Q. And wallets can be copied, right?
A. Yes. In theory, you could copy your wallet from a computer to a cell phone or from a cell phone to another computer.
Q. And you could share your wallet with someone else?
A. In theory, you could.
Q. And that person could share it with someone else?
A. Yes.
Q. So the wallet could be distributed to lots of people?
A. It could be, but it would defeat the purpose of a wallet.
Q. I'm just asking -- so aside from what you think the purpose is, I'm just asking, a wallet can be shared with lots of people?
A. Yes, it can.
Q. You talked for a moment about cryptojacking, and you described it as an intrusion without authorized access to the computer; is that right?
A. Correct. Cryptojacking is when you intrude upon a computer you don't have access to and you plant mining software to mine cryptocurrencies with that computer.
Q. But if you had access to the computer, and it wasn't an intrusion, then it wouldn't be cryptojacking, right?
A. If you had legal access to that computer and you were allowed to mine and use the resources of that computer, then, yes, it would be legal.
Q. I'm going to direct your attention to Exhibit 436.
MR. KLEIN: This has been admitted by the government,

Your Honor. So please publish.

Q. (By Mr. Klein) I'm directing your attention to the top of that exhibit.

A. Okay.

Q. The prosecutor asked you a series of questions about this exhibit, and that top portion, ETH/Monero?

A. Yeah.

Q. What's Monero?

A. Monero is another type of cryptocurrency.

Q. And you've seen no evidence of Monero in this case, have you?

A. I have seen evidence of Monero listed here in this document.

Q. But no other evidence; beyond this one mention of Monero, you've seen no other evidence of Monero?

A. No. I've not examined other evidence of Monero.

THE COURT: You don't know of any other --

THE WITNESS: I don't know of any.

MR. KLEIN: Let's turn to Exhibit 462, previously admitted. Sorry. 562. Penmanship is even bad for myself. 562.

Q. (By Mr. Klein) You looked at an exhibit -- the prosecutor showed you an exhibit talking about -- allegedly, my client talking about various things that could or were purchased by mining; do you remember that?

A. Can you please elaborate on that?

MR. KLEIN: One second. Sorry, Your Honor.

THE COURT: Take a moment to get it straight. That's fine.

MR. HAMOUDI: Thank you, Your Honor.

MR. KLEIN: Thank you.

502, please.

Q. (By Mr. Klein) Do you remember looking at this exhibit with the prosecutor?

A. Yes, I do.

Q. And do you remember discussing the text at the top about $5,000 a month?

A. Yes, I do.

Q. Okay.

MR. KLEIN: If you could keep this exhibit here, and also pull up 462. We're going to try a split screen.

THE COURT: It will work.

MR. KLEIN: The second page, please. Actually, page 0004. Sorry.

Q. (By Mr. Klein) Do you see this Exhibit 462, page 4? Do you see that on the right of your screen?

A. I do.

Q. And do you see what's alleged to be a discussion about things that might be purchased?

A. Yes, I do; designer clothes.

Q. Okay.

MR. KLEIN: Now I'm going to show you Exhibit 304. I don't know if we can do a triple split.

THE COURT: I don't think so.

MR. KLEIN: Then pull out and go to 304. 304 has been previously admitted.

Q. (By Mr. Klein) You're aware that the FBI arrested my client, correct?

A. I am aware of that.

Q. And that they went into her house in South Seattle that she shared with a number of roommates?

A. Yeah, okay, yes.

MR. KLEIN: We might be able to do it.

THE COURT: Maybe Luz can do it.

MR. KLEIN: Yeah. Thank you, Luz.

Q. (By Mr. Klein) That's a picture of her room, Special Agent.

A. Okay.

Q. Are you aware of any designer clothes ever being seized in the case?

A. No, I'm not.

Q. Are you aware of any cash being seized in this case?

A. No, I'm not.

Q. Are you aware of any drugs being seized off my client in this case?

A. No, I am not.
Q. I'm going to turn to Exhibit 801. This is the script that you were shown by the prosecutor; do you remember that?
A. Yes, I do.
Q. As far as you know, you don't -- you don't know that this script was ever run, do you?
A. I know that this script was taken from the computer off the premises of the suspect in this case.
Q. That's not my question.
You don't know that it was ever actually run, though, do you?
A. I do not know if it was ever run, but I know the address that was received -- received funds, yes.
Q. Can an address receive cryptocurrency from multiple sources?
A. It can, yes.
Q. So if I own an address, can anyone send me cryptocurrency to my address?
A. Anyone can send that, but I will be able to identify the sender of that cryptocurrency.
Q. Yeah, but -- so multiple people can send money to the same address?
A. Correct, but those multiple people will have different addresses.
Q. And when you set up a mining pool, can you designate which

address you want the mined cryptocurrency to go to?
A. Yes. So when a mining pool gets set up, cryptocurrency will go to the main address associated with that mining pool and then the account holder that signed up with the mining pool.
Q. And you can send the cryptocurrency to whatever wallet address you designate?
A. Whatever wallet address you designate.
Q. Thank you.
Turning now to Exhibit -- actually, turning now to Exhibit 316, which has been previously admitted -- I think my penmanship is better here.
THE COURT: We hope so.
MR. KLEIN: I should have been a doctor.
310. I was wrong. So my penmanship is bad. My 10s are 6s and my 6s are 10s.
Q. (By Mr. Klein) You understand these are gift cards -- I mean --
THE COURT: Yeah, yeah. They're obvious. They're gift cards. Ask a good question.
Q. (By Mr. Klein) And so you don't know how these gift cards were purchased, do you?
A. I do not, no.
Q. You don't know who purchased them?
A. No, I do not.
Q. Turning now to Exhibit 851. So what is this again?

A. So this is the block explorer that shows transactions made from Nanopool to the particular address.
Q. Okay. And that's the wallet address you previously testified about?
A. Correct.
Q. And that -- 852 is the next exhibit you testified about?
A. I would assume so, yes.
Q. We're going to pull it up. Sorry.
MR. KLEIN: Luz, can you please pull up Exhibit 852?
A. Yes.
Q. (By Mr. Klein) And then the prosecutor talked about -- and we're not going to pull these up -- 853 and 854, ultimately getting to your spreadsheet?
A. Correct.
Q. The text message you read earlier, what was the amount per month that was discussed in that text message?
A. I believe it was $5,000.
Q. And how many months made up your spreadsheet?
A. The span of about five months.
Q. Okay. And what would the total of 5,000 times five -- it's a little more than five, actually, I think, but let's say five. What would that total up to?
A. What was the time when that text message was sent?
Q. We can look at it.
A. Yeah, let's look at it.

Q. Well, let's start there. What was the total?
A. $10,014.
Q. Okay. And so that is not, just on its own, $5,000 a month?
A. That's correct.
Q. But your spreadsheet --
MR. KLEIN: Let's pull that up, which is 855.
MR. HAMOUDI: She's not going to be able to pull it up.
MR. KLEIN: One second, Your Honor.
THE COURT: Do you really need it?
MR. KLEIN: I think we're fine without it.
One second, Your Honor.
I'm just trying to find the exhibit number, Your Honor. I apologize.
One second.
Q. (By Mr. Klein) So this was sent in March?
A. Okay.
THE COURT: March of 2019.
A. March 24th of 2019?
Q. (By Mr. Klein) Yes.
A. Okay.
Q. To your knowledge, did the FBI seize any cryptocurrency from my client?
A. To my knowledge, no, I was not aware of that.
MR. KLEIN: Nothing further.

MR. FRIEDMAN: Very quickly, Your Honor.

THE COURT: Okay, Mr. Friedman.

REDIRECT EXAMINATION

BY MR. FRIEDMAN:

Q. Good morning, again, Mr. Kenney.

You were just asked a lot of questions about the possibilities of could multiple people put money into one wallet, could multiple people take money out of one wallet?

A. True.

Q. Okay. Would you take a look at Exhibit 436? The fourth text down, what does Ms. Thompson say she's doing?

A. She says in the text, "Just living with a friend and hacking EC2 instances and getting access to some AWS accounts and using them to mine crypto."

Q. You talked a moment ago about mining cryptocurrency being legal if you had legitimate access to an account, I think, and were allowed to do that?

A. That's correct.

Q. Does she say anything about that here, or how does she describe her conduct?

A. She describes it as hacking an EC2 instance.

Q. And you were asked a number of questions about -- relating to how much money was coming in, and was it $5,000 a month; do you recall those?

A. So it doesn't appear to be $5,000 per month, but I do know

that the message was sent in March, and most of this activity occurred after that message was sent.

Q. Okay. And do you recall reading another IRC chat, talking about how much money Ms. Thompson was making or could make?

A. Um --

Q. I'll ask you to look at Exhibit 462, page 5.

A. Ah, yes.

Q. In the first message there, can you see the date on which this was sent?

A. This was sent on 02:34:56.

Q. I threw you a little bit of a curveball. The date is right above that. That's a time, I think.

A. Oh, I see, yes, 2019-7-28.

Q. So a couple months after the earlier statement about $5,000 per month?

A. Correct.

Q. Do you see Ms. Thompson explaining how much money or why she's getting a certain amount of money from cryptocurrency money?

A. I see her explaining that she is doing "cryptojacking and I just don't have the motivation to run a full-fledged enterprise operation."

MR. FRIEDMAN: Thank you. I have no further questions.

MR. KLEIN: Just a few brief questions about the same

exhibits.

THE COURT: Okay.

RECROSS-EXAMINATION

BY MR. KLEIN:

Q. Both of those messages you were just shown were in July, right?

A. That appears so.

Q. You don't know who Ms. Thompson was talking with?

A. I do not, no.

Q. You don't know the circumstances behind those messages or how -- you don't know the circumstances?

A. I just know it says, "cryptojacking and I don't have the motivation to continue."

Q. You can just see what's in the message, though?

A. Correct.

MR. KLEIN: Thank you.

THE COURT: Okay. Thank you. You can step down. And the government's next witness?

MS. MANCA: Yes, Your Honor, the government calls Waymon Ho.

THE COURT: Mr. Ho, please raise your right hand and listen to the oath.

WAYMON HO,
having been first duly sworn, testified as follows:

THE CLERK: Please state your name for the record, and

spell it for the court reporter.

THE WITNESS: It's Waymon Ho; last name, H-o; first name is spelled W-a-y-m-o-n.

THE COURT: Thank you, Mr. Ho.

Ms. Manca?

DIRECT EXAMINATION

BY MS. MANCA:

Q. Sir, where do you work?

A. I work for the FBI.

Q. What do you do for the FBI?

A. I'm a computer scientist.

THE COURT: You know, I've just got to tell you. When I first started in the business, the FBI agents were big and burly and always white men. And it's so interesting to see the new FBI. And it's better, don't get me wrong, but I still have this reaction to expecting to see Elliott Ness and some of those characters.

But it's great. What the FBI has done is shifted a lot, both since 9/11 and the rise of computers and the like.

Go ahead, Ms. Manca.

Q. (By Ms. Manca) What does a FBI computer scientist do?

A. Yeah. So we do a variety of job duties in the FBI. I can boil them down to a couple of categories, one of the first ones being digital forensics.

So we examine digital evidence seized by the FBI, and we

extract data from them.
The second being incident response. So we provide assistance to victim companies when they may be a victim of a computer-intrusion event. We respond, and we help assist them with that.
We also do software development. So we create scripts and applications to assist the FBI.
And also we do threat intelligence, which is taking the data that we have access to at the FBI, and developing and identifying threats based off of that.
Q. How did you become involved in technology?
A. I started with a computer at a very young age, and my passion for computers kind of grew over time; learning how to, you know, build a computer and learning the software behind it led me to pursue a degree in computer science.
Q. Did you obtain a degree in computer science?
A. I did.
Q. From which university?
A. California State University Fullerton, or Cal State Fullerton.
Q. While you were working at Cal State Fullerton, did you have any jobs in technology?
A. Yes. I was an IT supervisor for the department at Cal State Fullerton, and I also did undergraduate research in computer science as well.

Q. And after you graduated, you joined the FBI?
A. I did.
Q. How long have you been with the FBI?
A. About five years now, as a computer scientist.
Q. Do you hold any professional certifications? We'll start with external.
A. I do, yes.
Q. What are those certifications?
A. These certifications are through an institute called SANS, through their Global Information and Assurance Certification program.
Q. What is SANS? What is that an acronym for?
A. SANS is a well-known institute that provides certifications in various topics, including cyber security, digital forensics, and incident response.
Q. And do you know what the acronym SANS stands for?
A. I do not.
Q. It is just known as SANS?
A. Yes.
Q. And what certifications do you hold from SANS?
A. I hold multiple, the first one being certified to reverse engineer malware; another is a network forensic analyst; another is incident handler; another one for intrusion analyst; a certified forensic analyst; and I believe that's all I currently hold.

Q. What about internal certifications?
A. I'm a certified instructor for the adjunct faculty program at the FBI.
Q. So as part of your job as an instructor for the FBI, who do you teach?
A. So I'm authorized to teach, on behalf of the FBI, to internal and external audiences.
Q. And when you first joined the FBI as a computer scientist, is there any training associated with that?
A. Yes. We have a two-month training that we take in Quantico, Virginia.
Q. Are you also a member of the CAT team?
A. Yes.
Q. What is that?
A. The CAT team or the Cyber Action Team is the FBI's cyber division's Rapid Deployment Response Team. As an operator myself, we are on-call 24/7 to respond to any critical computer-intrusion event in the world.
Q. How does someone join the FBI's CAT team?
A. It is a very selective and competitive process. There's only about 50 of us in the entire FBI. We have to compete and go through phases of examinations where we have to, essentially, investigate an entire computer-intrusion event from start to finish, alone.
Q. Have you received any recognition for your work?

A. Yes. I've received several special achievement awards, and on two separate occasions, the Medal of Excellence award, which is one of the highest awards at an FBI field office.

Q. How did you become involved in the investigation of Paige Thompson?

A. I had a request from Agent Martini to review some chat communications that were from Paige Thompson. It was kind of my job to translate that communication.

Q. Do you have that job a lot, translating things into English?

A. I do. Often, I look at technical data, and I translate it to, you know, either an agent or an intelligence analyst.

Q. Based on the online activity that you observed, did you have a basic understanding of Paige Thompson's hacking activity?

A. I did.

Q. And can you give us a general overview of the online messages that you reviewed prior to conducting any sort of search warrant?

A. Yes. So I reviewed communications that were on the platform Slack, as well as Twitter.

The primary goal for me was to identify any information that's related to the investigation, any information about how Ms. Thompson conducted computer intrusions onto victim companies, as well as identify any factors that may be pertinent for a search warrant at her residence.

Q. And how did the information that you reviewed inform planning about how the search warrant would be executed?
A. So the information from those communications provided me some things to look out for during the search; for example, there was screenshots in the chats that indicated a Linux operating system was running. There were chat references to encryption, as well as references to a kind of directory that contained aws-like dumps from victim data, as was mentioned before.
MS. MANCA: Agent, could you pull up Exhibit 408, which has already been admitted?
Q. (By Ms. Manca) Mr. Ho, this is Exhibit 408. Do you recognize that as a Slack communication you reviewed?
A. I do.
Q. And how did that relate to what you just testified about?
A. So I would take something like this from a communication and make sure that, you know, this information is communicated with the case team, especially the team that would also be part of that search. It's to identify that, you know, during the search, to look for this piece of data.
MS. MANCA: Thank you. We can take that down.
Q. (By Ms. Manca) So were you actually involved in executing the search warrant at Ms. Thompson's house in Seattle?
A. I was.
Q. And when you were at the house, what did you do?

A. My primary role is a searcher, specifically for the technical information, as well as the digital devices that were present in her room.
Q. And when you're locating a digital device, what are you concerned about, or what are you trying to do in that moment?
A. The main goal is the preservation of that digital evidence in its original format.
Q. How do you -- so if we take you back to the scene of the house, what was the state that you found that computer in when you got there?
A. Are you talking about the white desktop?
Q. Oh, yeah, let's go -- yes, let's, actually --
MS. MANCA: Could you put up Exhibit 305?
Q. (By Ms. Manca) Do you recognize what's shown in Exhibit 305?
A. I do, yes.
Q. What is it?
A. It appears to be a custom-built, white, desktop computer.
Q. And is that the same computer that you located during your search?
A. Yes.
Q. What was the state of that computer when you got into that bedroom?
A. It was powered on.
Q. If it's powered on, what does that allow you to do from a

forensic perspective?
A. So that allows me to preserve evidence in that live environment, particularly live memory. It's also known as RAM, or random access memory. This type of digital evidence is considered volatile, which means that if the device is powered off, that information is no longer there.
Q. And when you powered on the device, you mentioned you were looking for a specific set of files; is that right?
A. I didn't power on the device; it was already on. But I was looking for a specific set of files.
Q. Okay. Sorry about that.
Did you locate the specific files that you were looking for?
A. I did.
Q. Can I show you Exhibit 307? Do you recognize what's shown in 307?
A. I do.
Q. And what's the file directory of those files?
A. So during the search, I identified that there was a mounted network share. It was labeled "export_one," and inside that network share there was a folder called "aws_dumps."
Q. And what did you do once you found that file directory and these files on that computer?
A. I had the FBI photographer take a picture of the screen, as shown here in the exhibit, and then I proceeded to preserve that digital evidence.

Q. What did preserving that digital evidence consist of?
A. So that would mean obtaining a copy of that live on that device. So I would connect a forensically wiped media drive onto that device, and then copy the content of that folder over to it.
Q. How long did it take to do that?
A. I don't have a precise time, but an estimate would have been a couple of hours.
Q. How much data are we talking about here being captured?
A. I'm not sure on the exact amount, but it is definitely hundreds of gigabytes, if not closer to a terabyte.
Q. Can you give a sense of how big a terabyte is, like, related to, maybe, the storage on a laptop, a conventional laptop?
A. Yeah. So one terabyte is about 1,000 gigabytes. If you're taking a general consumer laptop that is about 256 gigs of hard drive space, it's about four laptops.
Q. Did you seize any other devices from that bedroom?
A. I did.
Q. Which devices?
A. There was a laptop device, a phone device, and several other devices in that room.
MS. MANCA: Can we see Exhibit 308?
Q. (By Ms. Manca) Is that the laptop that you seized?
A. Yes.

Q. And was that later given an evidence number 1B-2?
A. Yes.
Q. And the large, white, desktop computer, was that later given an exhibit number by the FBI?
A. Yes, it was 1B-52.
Q. Okay. Where did the devices go after they were seized?
A. So the evidence items are packaged by the evidence handler at the scene, and then transported to the main FBI field office to be placed in the evidence control room.
Q. Have you physically examined these devices that we're talking about?
A. I have, yes.
MS. MANCA: Can we, actually, pull up Exhibit 305 again?
Q. (By Ms. Manca) So when you physically examined Ms. Thompson's desktop computer, what did you notice about it?
A. I noticed that it was a very, very large computer. The picture actually doesn't really do it justice on how large it is. It's kind of like -- like this large, this tall, and this wide. So think of, like, several desktop computers, even large ones, kind of piled together into one large machine.
Q. And you're putting your hands about four or five feet apart and then maybe two feet, and then three feet, in a cube?
A. It's like a rectangle instead of cube, yeah.
Q. What else did you notice about the physical aspects of this

device?
A. That it contained a significant amount of hardware, including a large amount of hard drives, as well as other hardware that's not typically found in consumer desktop computers.
Q. Did you get a sense of whether this was a custom-built computer or whether it was off the shelf?
A. I did get a sense that it was custom built.
Q. And approximately how much storage capacity was there on this computer, if you know?
A. I can speak to some of the volumes that were identified on the desktop computer, but I don't know the full amount. There was one RAID array that was about six terabytes in size. There was another that was about 11 terabytes in size. Aside from those two volumes, there were several other volumes. So I'd say it's north of 18 terabytes.
Q. Are you familiar with the concept of a digital image?
A. I am, yes.
Q. What is that?
A. So a digital image is like a byte-for-byte copy of a device, like a physical device. For example, taking the hard drive out of a computer and creating that in a digital form to review.
Q. Is that how you reviewed the devices in this case, the desktop computer and the laptop computer?

A. Yes, digital forensic copies were made.
Q. Why don't you just power up the computer again and start looking through it?
A. Yeah. So our policy, as well as just a forensic practice, is not to alter the original in any way or form.
When you turn on a device, even as it's loading into the log-in screen, there are many changes that are happening in the background that make changes to the device. So we tend not to alter the original evidence in any way.
Q. How do you know that the digital forensic image you're reviewing is an exact copy of the contents of the digital device?
A. So we verify through a number of methods, but one of the main ones is through a hash value.
Q. What is a hash value?
A. So a hash value is kind of a digital unique fingerprint of a piece of digital evidence, whether it be a file or an image of a computer. It's represented as a series of numbers and characters, and it uses an algorithm to determine that string of, you know, numbers and letters that represent the uniqueness of that specific digital evidence, so that the content of it, as it is when it is hashed, generates that unique value.
Q. How big of a change do you need to make to a computer to change its hash value?
A. Any change in the content would result in a drastic change

of the hash value. Adding a space somewhere, adding a small file, deleting a file, those changes, even turning on the computer, even not doing anything else with it, will result in a change.

Q. So if you compare the hash value of the forensic image that you have to the hash value of the digital devices and they match, what does that tell you?

A. That tells me that is an original -- or it contains the data from the original evidence, and it matches.

Q. Did you compare the hash values for the both desktop computer and the laptop computer?

A. I did.

Q. And what was the result of that comparison?

A. They matched.

Q. And what did that tell you?

A. That tells me that the digital forensic image is a copy of the original, no alterations.

Q. Did you use any forensic computer tools to examine the digital image?

A. I did. I used a variety of FBI-approved forensic tools.

Q. Can you describe what some of those tools are?

A. Yes. One of the tools is called X-Ways. You may have seen it in the other exhibits in that screen. I also used other tools that are used on Linux operating systems.

Q. Are these tools accepted by the FBI for use by its forensic

computer scientists?
A. Yes.
Q. And are they generally accepted in the field of forensic computer examination?
A. Yes.
Q. Were either of the devices, the desktop computer or the laptop computer, encrypted?
A. They were.
Q. How did you decrypt them?
A. The decryption key was provided to Agent Martini during an interview with Ms. Thompson, and that key was provided to me to decrypt the image.
Q. Can you give us a general overview of the information you found on Ms. Thompson's computer? I'm going to talk about the desktop computer. So a general overview of the items you found on the desktop computer when you searched it.
A. Yes, so I identified a large number of things in various categories, one of them being communications, so messages and other types of Internet data, web history. I also found scripts and applications that were used to conduct computer intrusions, as well as victim data that was identified on the device.
Q. Did you get a sense -- is one of the things you look for when you're examining a computer evidence about who used the computer?
A. Yes. One of the things I look for is ownership of that

device, if there were multiple users, and other underlying information.

Q. What did you find when you examined Ms. Thompson's device for user information?

A. Aside from, you know, the default, like root or administrator account, there was only one other user account. That one was named Erratic, E-r-r-a-t-i-c.

Q. And based on your review of Ms. Thompson's device, who were the primary user or users of the computer?

A. It appeared to be Ms. Thompson, based off the --

Q. Did you have evidence of any other users?

A. I did not.

Q. What screen names or user names did you see in the computer?

A. There were multiple references to Erratic, to Molly, M-o-l-l-y, to Paige or Paige Adele Thompson.

Q. Did you understand what "Molly" is or refers to?

A. I do not, no.

Q. You also mentioned that you had looked at IRC, or Internet Relay Chats, or you looked at communications?

A. Yes, I did.

Q. What kind of communications?

A. So there were the IRC, or Internet Relay Chats, some Slack communications, as well as Jabber communications.

Q. How were these communications stored on Ms. Thompson's

devices?
A. So they were stored as log files or history files on the users directory in the Erratic user directory.
Q. Once you located these communication logs on Ms. Thompson's devices, did you make a copy of them?
A. I did. I forensically extracted them from the device.
Q. And to whom did you give a copy of those communications for further review?
A. I provided it to the FBI case team.
Q. Did that include Zach Hansen?
A. It did.
MS. MANCA: Your Honor, at this time, I have a series of exhibits I'm going to list. I provided the court clerk with the list of exhibits. I'm going to seek to admit them in bulk.
So out of the 600 series, Exhibits 602 to 612, 621 to 624, 640 to 647, 670 to 677.
From the 700 series, 701, 710, 730, 740, 750, 760, 780 to 782.
And from the 800 series, 800 to 812.
Q. (By Ms. Manca) Mr. Ho, have you, prior to your testimony today, reviewed the exhibits that I just listed?
A. I have.
Q. Can you give us an overview of what these exhibits are?
A. So these are files or file listings for content that was extracted from the forensic images that I reviewed from

Ms. Thompson's residence, primarily the desktop computer labeled as 1B-52 and the laptop labeled as 1B-2.

Q. And who created these copies?

A. I did.

Q. And can you tell us what format these documents are in?

A. They range in a variety of different file formats, but some include text files, log files, programming scripts, as well as others.

Q. And did each of these exhibits fairly and accurately represent the content of Ms. Thompson's computer?

A. Yes.

MS. MANCA: Your Honor, I move to admit the exhibits that I just listed.

THE COURT: Are you ready to address this now, Mr. Klein, or do you want some time?

MR. KLEIN: Your Honor, I think we're not objecting, but there is just a lot of them, and I just want to double-check.

MS. MANCA: I can --

MR. KLEIN: The lunch hour, Your Honor, is that okay?

THE COURT: But we want to keep going. If you see one that causes an issue, let me know.

MR. KLEIN: I will, Your Honor.

THE COURT: Otherwise, go right ahead, Ms. Manca.

MR. KLEIN: Yes.

MS. MANCA: Thank you, Your Honor. Just thought I'd avoid us stopping and starting a lot, so thank you very much. Can we go with Exhibit 602?

Q. (By Ms. Manca) And I'm going to be showing you Exhibits 602 to 608. Do you have a general sense of what this category of exhibits is?

A. Yeah. So this is a directory tree or a file directory listing of some of the contents that were identified on Ms. Thompson's devices.

Q. Where was this file directory located?

A. So this one was found on her desktop computer, and one of the volumes -- one of the large RAID volumes called md126, and this is in the home folder under the user Erratic, and there was a folder in that user directory folder called aws_hacking_shit.

Q. Can you give us an overview of the types of files and folders that you located within this directory?

A. That folder contained a large number of scripts that appear to be designed to use to exploit or conduct intrusions against Amazon AWS environments. It contained some victim data, as well as some log-in history that's related to AWS.

Q. What was the significance of this file directory relative to other file directories you reviewed on her computer?

A. This contained a lot of tools and methodology that was used to conduct intrusions against AWS victims.

MS. MANCA: Can we pull up 603, please?

Q. (By Ms. Manca) Could you tell us what this is?
A. Yeah. This is a file directory listing of a folder called aws_scanner.
Q. Where was this located?
A. This was located in the home directory of the Erratic user.
Q. And what was the significance of this file path?
A. It contained a couple of scripts for conducting scanning, but also there was a script in there called aws_session.sh, which is one of the scripts that is used to authentication into AWS.

MS. MANCA: Can we pull up Exhibit 604?

Q. (By Ms. Manca) Can you tell us what is Exhibit 604?
A. This is a listing of the .aws folder that was identified in the Erratic home directory. The .aws folder contains information about the configuration and the credentials that are used with the AWS Command-Line Interface or CLI application.
Q. And Exhibit 605, do you recognize this?
A. Yes.
Q. Can you tell us where you found this?
A. Yeah. This was identified on her white desktop computer. It's the aws_dumps folder.
Q. And you testified earlier about a file directory you captured in live memory and viewed on the screen. Is this the same file directory?
A. Yes.

Q. Exhibit 606, can you tell us what's in Exhibit 606?
A. Yeah. This is a folder called "miner." It was located in the aws_hacking_shit folder, and in that folder this miner folder contained scripts related to cryptocurrency mining.
Q. And Exhibit 607, what is this?
A. This is a folder called .ssh. This was identified in the Erratic user directory. The contents of this contain information related to the application SSH.
Q. What is the application SSH?
A. "SSH" stands for "Secure Shell." It is an application that's primarily used on Linux operating systems, which allows the computer to remotely connect to another computer.
Q. How does one computer remotely connect to another computer through a Secure Shell connection?
A. There is a large amount of factors, but a Secure Shell connection requires a connection directly between two computers using a specified port. This port is commonly port 22.

It creates an encrypted tunnel between the two, and there is an authentication process that occurs. Two of the common methods of authentication are a user name and password, or a key pair, a public and a private key.
Q. And "rsa" appears in a lot of these file names. Do you know what rsa is?
A. Yes. The files ending in id_rsa are the keys that are used for that key-pair authentication through SSH.

Q. So based on your review of this folder, are you able to draw any conclusions about what these file names mean or their significance to Ms. Thompson's activity?

A. Yeah. So these files appear to be keys that are specified for specific IAM Roles. So it may have been used to directly connect to certain AWS victims.

Other files in there include the configuration information, which provides information on how the SSH application is configured to connect to certain computers, and the note hosts file in that folder also describe which computers that specific desktop computer ever connected to.

Q. So based on these files and folders that you just testified about, are you able to draw a conclusion about whether Ms. Thompson actually, in fact, connected to other devices through this mechanism?

A. So this folder definitely provides evidence that is indicative of a secure connection or shell connection to a victim, but I'm not sure if I'm able to fully verify that just on this alone.

Q. What additional information would you need to verify whether that connection had been made?

A. Typically, that would be to obtain information or logs from the recipient or the other remote host, or any logs that would determine that a connection had been made.

Q. I'm going to talk to you about Exhibit 608. Do you

recognize that?
A. Yes.
Q. Can you tell us what it is?
A. This is a file called aws.commands. It was found in the home directory of the user Erratic on the desktop computer.
Q. And what are all these lines that we see?
A. So this appears to be sort of a command history log. So on Linux operating systems, every command that you type can be preserved in a history file. This is typically called a bash history. So if you've seen, like before in a TV show or a movie, where, you know, there's, like, a black screen and somebody is typing a command and they press enter, once that "enter" is hit, that command that was typed gets saved somewhere. It's kind of a log that provides history of commands that were run on a system.
Q. Is this the same as a keystroke log?
A. No. A keystroke logs every single thing you type on a keyboard. This only logs the command. So if I type something on a keyboard through a keystroke log, and maybe I backspace and add some stuff after, that will get captured in a log. This only captures the commands that were submitted.
Q. Do you have a sense of whether this log was manually created or automatically created on Ms. Thompson's device?
A. I believe this one was manually created. At very end of this file also provides some evidence of that as well.

Q. And did Ms. Thompson save every single command that she ran?
A. Not to my knowledge. No. I don't know if she did or not.
Q. Who decided what information would be included in this log?
A. It would be the user that generated this log.
Q. And how did this document or the information in this log inform your analysis of Ms. Thompson's computer?
A. Yeah. So this file provided me a series of commands that may have been ran on a victim system. So, typically, this would give me kind of a timeline of events that occurred. Of course, there's no timestamps. The order of the commands may not be the way it is, but I can infer from this log file a series of commands that were run, you know, from the authentication of a connection to an AWS victim, and then subsequent commands that would be run on that system.
Q. And have you seen consistencies between this log and other evidence that you've reviewed in the case, such as information you've obtained from victims or scripts you found elsewhere on the computer?
A. Yes.
Q. Based on your review of Ms. Thompson's computers, were you able to determine the steps of her hacking process?
A. I have.
Q. Can you describe those steps or stages?
A. Yeah. So in a very rough or general overview of these

steps, there's multiple involved, but the first one involves, you know, what's been referred to before as the "proxy scanner" to identify if an AWS system is able to be exploited or is vulnerable to a type of attack known as a server-side request forgery attack.

Once Ms. Thompson is able to scan and identify these vulnerable hosts, the next action is to gather information about that specific server or host. So that would be -- and then it's been explained before -- to gather the name of the IAM Role that the exploited or vulnerable server has, and then using that to do a third step to authenticate into an AWS environment using those credentials. It's a multistep process.

Q. And once Ms. Thompson was able to authenticate in with these credentials, what additional steps did she take after that?

A. Yeah. So that can be kind of explained in two different parts. The first one is commonly referred to as "reconnoissance activity." So this is gathering information when you're in a system, so commands, like, describe instances or list-buckets, you're essentially gathering information about the environment that you just got into.

The second is, of course, the data-theft syncing of buckets, copying data over, and other post activity, including, you know, creating new servers, creating new security groups; essentially, things that make changes to a system.

Q. So we're going to run through all of these steps, but first I want to talk to you about the concept of anonymization.

What kind of records are available when one computer connects to another computer over the Internet?

A. There's information that gets saved when that happens.

At a network level, that type of packet information could be logged. If you're talking about connection information between two computers, especially if you're sending information to, for example, a web server or a different server, that server can see which IP address you're coming from; other information such as, you know, what device you came from, what time, and other things like that.

Q. Are there ways to anonymize or disguise where you're coming from on the Internet?

A. There are.

Q. What are some of those ways?

A. One of the more common ones is a VPN, or a Virtual Private Network. What that allows you to do is to connect to a VPN server through an encrypted means, usually, and allow your computer to simply forward that traffic to the VPN server, in which that VPN server would then forward your traffic to wherever you're trying to go.

Q. Is there anything illegal about using a VPN?

A. No.

MS. MANCA: Can you display Exhibit 112 without

publishing?
Q. (By Ms. Manca) Would Exhibit 112 help you explain what a Virtual Private Network or a VPN is?
A. Yes.
Q. Does this fairly and accurately describe what it is?
A. Yes.
MS. MANCA: Your Honor, offering Exhibit 112.
MR. KLEIN: No objection.
THE COURT: 112 is admitted.
(Government Exhibit 112 admitted.)
Q. (By Ms. Manca) So can you walk us through this diagram from left to right?
A. Yeah. So on the left-hand side, you have your client, the host, and in the middle here, you have a cloud that is representative of a VPN server. And then on the right side, you have a computer that's your intended recipient.
So when you set up a VPN, you are creating -- if you look from the left device to the middle device -- an encrypted tunnel that contains encrypted content going from your computer to that server.
This allows anonymization because, for example, your Internet service provider, like Comcast, for example, can't see what you are doing. It can only see that you're communicating with one VPN server.
When a VPN server receives information through that VPN, it'll

then identify where to route it to, and that data will be sent to the recipient.

When the recipient receives the data, it will see that it came from a VPN server, but it may not know where it came from originally.

So that recipient will send data back to the VPN server, and once the VPN server receives that response, it will know to route it back to the client or host computer.

Q. So what does the server on the far right know about the computer on the far left, in terms of its IP address or identity?

A. It doesn't know anything. It only knows that it came from a VPN server.

Q. Do you know what iPredator is?

A. Yes.

Q. What is it?

A. It's a type of VPN service.

Q. So where would a VPN service like iPredator be depicted on this diagram?

A. It would be depicted in the middle, in that cloud environment.

Q. How many people are using the same iPredator IP addresses?

A. I don't know the answer to that, but typically, with a VPN server, there are anywhere ranging from dozens to hundreds to thousands per server.

Q. Can you explain what The Onion Router, or TOR, T-O-R, is?
A. Yeah. So TOR is another type of anonymization tool that allows you to move through a series of computers to encrypt your traffic.
MS. MANCA: Can we put up Exhibit 113 without publishing?
MR. KLEIN: We have no objection to this exhibit, Your Honor.
THE COURT: Okay. 113 is admitted. Thank you.
(Government Exhibit 113 admitted.)
THE COURT: Ms. Manca, we'll make this the last subject before lunch.
MS. MANCA: Okay. Thank you.
Q. (By Ms. Manca) So can you walk us through this drawing, similar to the way you did Exhibit 112?
A. Yeah. So when you are connecting through TOR, your computer, just like how you connect to a VPN, creates an encrypted tunnel. As you can see in the line -- with the solid line that says "encrypted by TOR."
And the reason why it's called an Onion Router is because, as it's moving through the TOR network, each of the TOR nodes doesn't know anything about the previous or the original sender. It only knows where to move forward to.
So you can think of it as, you know, I have a piece of paper that I close in a box, and then I close it in another box

and another box and another box. The final box that has, you know, this nesting, you know, boxes within it, I give it to one person; that person receives that box and says, okay, it came from you, this address says I need to give it to this other person; I'll give it to them; and then from there, that person receives the package, they open the box, take the box out, and sees the next destination it needs to give it to, and so forth.

This is kind of like the reference to the onion part, it's peeling back the different layers each time. And once it heads to the recipient of where it's intended to go, that traffic gets provided to that server unencrypted, at least the actual method of travel itself is unencrypted.

The content can be encrypted, but that -- it's the same as a VPN at that point. The end recipient would only see that it came from some TOR server, but no other information about the original sender.

Q. Is TOR legal?

A. It is.

Q. What does the computer on the right of this drawing know about the computer on the far left?

A. It does not know anything.

Q. Can I show you Exhibit 406, which has already been admitted, and zooming in on the bottom message.

Is this a Slack communication that you reviewed during this investigation?

A. Yes.

Q. And there's, in that second line, "I'm like iPredator, TOR, S3 on all of this." What did you interpret that to mean based on your review of Ms. Thompson's devices?

A. So what I see here is that she is using this method of her device connecting to an iPredator VPN, through that iPredator VPN connection connecting to TOR, and then from there, using TOR to connect to Amazon Web Services.

MS. MANCA: I think that's probably a good place to stop.

THE COURT: We're going the take our lunch break a little earlier because I have some scheduling matters to go over with the lawyers. Go ahead and take a little extra time. I'll ask you to be back by 1:20. So be back at Judge Pechman's courtroom at 1:20.

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: Mr. Friedman, you had a couple of items you wanted to bring up?

MR. FRIEDMAN: Your Honor, I think one has been resolved.

What that does leave is, two of the government's witnesses next week will be testifying remotely, and I think both parties agree about that, but we think it would be helpful to have, on the record, Ms. Thompson's agreement or waiver of her right to

confront in person.

THE COURT: Which two are they?

MR. FRIEDMAN: Those would be Clint Popetz and Eric Brandwine.

THE COURT: It says Eric Brandwine is a possible witness.

MR. FRIEDMAN: He is now a definite witness. "Possible," I think, was possibly for that date. He's definite.

THE COURT: And by "virtual," are you talking about virtual live?

MR. FRIEDMAN: Live, yes.

THE COURT: Okay. Victoria, do we know that?

THE CLERK: Yes.

THE COURT: And we're going to be set up for it?

THE CLERK: Yes.

THE COURT: Mr. Hamoudi, have you talked to Ms. Thompson about the right-to-confrontation clause and her right to have the witnesses here live?

MR. HAMOUDI: I have, Your Honor.

THE COURT: And has she agreed to do it in this manner?

MR. HAMOUDI: She has.

THE COURT: All right. Ms. Thompson, is that right?

THE DEFENDANT: Yes, Your Honor.

THE COURT: All right. We got that on the record.

MR. HAMOUDI: Thank you, Your Honor.

THE COURT: In regard to Dr. Muscatel, that "possible" is not date, that's -- you're not sure you're going to call him, right?

MR. FRIEDMAN: Well, I think that has to do partly with the question of whether the defense is presenting that type of evidence.

THE COURT: Yeah, okay. So you're intending to rest sometime probably on Tuesday?

MR. FRIEDMAN: That would be my guess, Your Honor.

THE COURT: And, of course, you don't have to commit to whether you're going to present a defense or not, but if you do present a defense, it would be, likely, a day or two?

MR. HAMOUDI: Two days, Your Honor.

THE COURT: Okay.

I think, though, if -- Dr. Muscatel is not going to be -- isn't he more, like, if they present -- if Ms. Thompson testifies or if they present their mental health expert?

MR. FRIEDMAN: That's the most obvious way in which he would testify, so. I think we probably just need to speak with the defense and get clarity on that issue.

THE COURT: But they don't need to tell you that until you rest.

MR. FRIEDMAN: Right.

THE COURT: So if you want to do it sooner, let us

know; otherwise, you don't have to.

MR. HAMOUDI: At some point, with respect to Dr. Goldenberg, who would be our mental health expert is -- I need to think on it, Your Honor, but I need some guidance from the court about scope, relevancy, and substance. That would be helpful. What's the best way to provide information to the court to get that direction?

THE COURT: Well, we can try to talk about it at a certain time, if you want to.

MR. HAMOUDI: That would be fine, Your Honor. Maybe the day before they rest, maybe we can --

THE COURT: Sometime on Monday. Okay.

MR. HAMOUDI: Thank you, Your Honor.

MS. MANCA: Your Honor, related to that discussion, the Court had talked about, I believe, a written order regarding John Strand's testimony and limitations related to that.

He is an anticipated witness for, maybe, late Monday, early Tuesday, and so it would help to go into the weekend knowing the scope of that testimony as well.

THE COURT: Okay. I'll try to do that for you.

MR. HAMOUDI: And the secret service agent, you know, I think it's Mr. Henderson?

MS. MANCA: Mr. Henderson.

MR. HAMOUDI: We have a pending issue.

THE COURT: Okay. I'll try to get to that.

MR. HAMOUDI: Thank you.
THE COURT: Okay. Let's --
MR. KLEIN: Your Honor?
THE COURT: Yes?
MR. KLEIN: There were some exhibits that are coming up that we do have objections to.
THE COURT: Oh, yeah.
MR. KLIEN: 115, 116, and 121. I'm happy to explain the objections, if Your Honor would like, now.
THE COURT: Those are the ones that are going to be brought up with Mr. Ho?
MS. MANCA: They are, Your Honor. They're demonstrative.
THE COURT: They're are what?
MS. MANCA: They're demonstrative, not substantive, computer exhibits.
THE COURT: So you're not going to offer them into evidence, but you want to display them as a demonstrative?
MS. MANCA: That's correct.
THE COURT: Are you all right with that limitation?
MR. KLEIN: Well, we still would object to them, but it's better.
THE COURT: All right. What is objectionable about them?
MR. KLEIN: No. 115 we think is argumentative; No. 116

deals with the SSRF attack. We still maintain our objections to evidence about that; and No. 121 we think is also argumentative.

THE COURT: Argumentative is not an objection that would keep it out, because it is demonstrative only.

116, you say there is no evidence to support it?

MR. KLEIN: Our objection, Your Honor, is a 403 objection, for right now. I'm not sure what all of it they're going to put in, but for the moment it's just limited to 403, is that it will sow confusion talking about it as a server-side request forgery.

THE COURT: Got it. Okay. I'll allow it, but I understand where you're coming from. For demonstrative purposes only, you can present it. Okay.

MR. KLEIN: Your Honor, when they put those in, will you make an instruction just so the jury understands they're not actual evidence?

THE COURT: Sure.

MR. FRIEDMAN: Can I raise one other issue?

THE COURT: Sure.

MR. FRIEDMAN: It appears that the defense, in its case, wants to call a number of witnesses from Capital One. That presents scheduling or difficulties, because all of those witnesses are on the East Coast.

THE COURT: Sure.

MR. FRIEDMAN: One is actually in Europe with COVID.

And so I think there's an agreement between the defense and Capital One that witnesses could testify remotely. If that's the case, the government will not object to that.

And we have a lawyer from Capital One that was hoping for -- who may want to address the court and ask for advisement.

THE COURT: I'll be very surprised if the defense is actually going to call any witnesses from Capital One, but --

MR. FRIEDMAN: They tell us they are.

MR. KLEIN: You might be surprised, Your Honor.

MR. FRIEDMAN: For schedule purposes, it's presenting a lot of issues for Capital One. Can Mr. Pastore, from Capital One, address the court?

THE COURT: Okay. Can you be in a position to tell us about that later today?

MR. KLEIN: Yes. One of our issues was, we were waiting for Mr. Ho's testimony to come in to make final decisions. So we've communicated with them. We've narrowed down our list dramatically, Your Honor, to four people from a much bigger list. So we're doing the best we can, and we've been in constant contact with Capital One's attorneys. We just haven't made a final decision.

THE COURT: Okay. But you may know more after Mr. Ho's testimony?

MR. KLEIN: Yes, Your Honor.

THE COURT: That's fine. Okay. Great.

Mr. Pastore?

MR. PASTORE: Your Honor, Jim Pastore, Debevoise & Plimpton.

I think Your Honor just hit the nail on the head, and, perhaps, we can table this.

We have been working cooperatively, but particularly with the witness with -- with COVID, to have them doing testimony may, first of all, I think, be quite an imposition, but, second, there may be ways we can be efficient, and to the extent they need information, we can work on stipulations with the government.

So I think Your Honor has hit the nail on the head. If we can just get more clarity and enlist the Court's help in doing that by the end of day so we know whether or not these folks need to travel or set up remote arrangements, we'd very much appreciate it.

THE COURT: Okay. As long as we keep working cooperatively in this way, we can get through this together.

MR. PASTORE: Thank you.

THE COURT: Thank you, Mr. Pastore.

Okay. Let's go to lunch. Please be back and ready to go at 1:20.

(Court in recess 12:00 p.m. to 1:29 p.m.)

THE FOLLOWING PROCEEDINGS WERE HELD
IN THE PRESENCE OF THE JURY:

THE CLERK: Please rise. This court is again in session.

THE COURT: Please be seated.

We'll continue with direct examination of Mr. Ho by Ms. Manca.

MS. MANCA: Thank you, Your Honor.

Q. (By Ms. Manca) Mr. Ho, over the break I showed you Exhibit 505, which has already been admitted. It was a GitHub Gist. Do you recall that?

A. Yes.

Q. Okay. Is that a document that you reviewed in the course of your investigation?

A. Yes.

Q. Did that refresh your memory about who or what the name Molly means?

A. Yeah. So the Molly part in the gist based on the context of that document shows that it's the name of the computer.

Q. Getting back to this concept of TOR and VPNs, did you find evidence that Ms. Thompson used a virtual private network or VPN?

A. I did.

Q. Do you have water? Do you need time to --

A. I have water, yeah.

Q. What VPN service did she use?

A. IPredator.

Q. And where did you find that evidence?
A. It was identified in a virtual machine that was located on Ms. Thompson's desktop computer.
Q. And what about TOR, did you find evidence that she also used TOR?
A. Yes.
Q. Where did you find that evidence?
A. In the same machine.
MS. MANCA: Agent, can we call up Exhibit 621?
Q. (By Ms. Manca) There's a category of exhibits --
MS. MANCA: And, Your Honor, my understanding is that these are all -- you know, I've offered these. I'll show them to the jury, with the Court's understanding, and then Mr. Klein will object to anything --
THE COURT: I don't -- you probably had an opportunity to review them and there's no objection to the exhibits as designated by Ms. Manca?
MR. KLEIN: Not now, Your Honor, yes.
THE COURT: Okay. Great.
So we can display 'em.
MS. MANCA: Okay. Thank you.
And are they offered --
THE COURT: They're all admitted into evidence. Thank you.
MS. MANCA: Admitted. Thank you.

(Government Exhibit 621 admitted.)

Q. (By Ms. Manca) All right. So I'm going to orient, because we're going to be looking at a lot of sheets that look like this, can you tell us what we're seeing in this screenshot?

A. In this screenshot, it's files in a folder called "client," and that folder "client" is within another folder called "openvpn." So this is some configuration information for the iPredator VPN from that virtual machine that I mentioned earlier.

Q. Okay. And is this what your screen looks like as you're sitting down doing your forensic examination?

A. Uhm, sometimes it is like this. This is using the forensic tool X-Ways.

Q. Okay. What's the other way it can look like if you're doing other examination?

A. Sometimes I use tools that involve the use of the command line. So as I mentioned earlier where, you know, typically the screen is black and there's like text on the screen and I type commands.

Q. Thank you.

MS. MANCA: Can we pull up Exhibit 622?

Q. (By Ms. Manca) Actually, so what is Exhibit 622?

A. 622 is a log or an excerpt of a log that was identified in the virtual machine that had the iPredator VPN set up.

Q. And what was the significance of this particular VPN to --

I'm sorry, this particular IP address to your investigation?
A. Yes. So this IP address at -- was logged on April 17th. This IP address is one of the IP addresses that Capital One had identified as conducting an attack against their system. And that IP address was observed by Capital One on April 19th.
If you look at the last line of this exhibit, it shows the same IP address still in use during that time.
Q. Okay. And is -- your testimony is essentially the same as to Exhibit 6223 -- I'm sorry, 623 and 624?
MS. MANCA: We can display those quickly.
A. Yes.
Q. (By Ms. Manca) And then 624?
A. Yes.
MS. MANCA: Okay. And then if we can go back to 621?
Can we go to page 2?
And page 3.
And page 4.
And page 5.
Page 6.
Q. (By Ms. Manca) Can you describe what this, you know, suite of pages relates to?
A. Yes. So these are configuration information for the iPredator VPN. It's a series of files that help set up a VPN connection using iPredator.
In one of the exhibits, you also saw there was an

authentication or credentials, user name and password, that is also used to authenticate into iPredator.

One of the files in there as well, the iPredator.conf or configuration file, is also a file that was -- is uploaded onto GitHub on one of the gists on Ms. Thompson's account.

Q. And we're not going to go into detail on each of those lines of code, but based on your review of Ms. Thompson's computers and these codes that we've just talked about, what did you determine about the way that Ms. Thompson's computers were configured to use iPredator and TOR?

A. Looking at these exhibits and as well as other information on the device, I determined that this specific virtual machine that was used to set up iPredator and TOR was used to redirect traffic coming from either her computer or computers within her network to connect to an iPredator VPN server or to go through TOR to conduct Internet activity.

MS. MANCA: Okay. Agent, can we pull up Exhibit 114.

And, Your Honor, I offer Exhibit 114 as a demonstrative.

THE COURT: 114 is admitted as a demonstrative exhibit. It means it doesn't go back to the jury room with you, but it helps the witness explain what he's talking about.

(Government Exhibit 114 admitted.)

Q. (By Ms. Manca) So can you walk us through from left to right on this drawing?

A. Yeah. So in the beginning, your devices and your home

network is serviced by an Internet service provider. So you have the home Internet coming into your residence.

In this section here is a slew of machines that are at your residence. And there's a computer right in the middle, a laptop to the left, and several other smaller computers around that are connected to that larger computer.

What those smaller computers represent are virtual machines. Virtual machines are simply a virtualized version of an operating system running on your physical computer. So what that means is let's say I'm running a Windows computer on my main computer, but I want to run Linux operating system, but I don't want to install another operating system, I'll run a virtual machine, which is kind of like a virtual server or virtual kind of machine that runs on its own using the resources of my physical hardware, and in doing so give me access to another set of -- you know, essentially another computer to use.

Depending on your resources and how -- how much resources a computer may have, you can spin up multiple virtual machines and have them all running at the same time. You can also set it up so that they talk to each other. So you can have this network ecosystem of machines all in one computer.

Q. Did Ms. Thompson have that network ecosystem on her computer?

A. Yes.

Q. There is -- going above the desktop computer, so you've got

the smaller computers, and then there's another computer in the middle right by the tunnel that goes out of the cloud on the left; what does that computer represent?

A. That represents that virtual machine I talked about earlier that had iPredator and TOR set up on that virtual machine.

What this shows here is that there's -- it's available there for the surrounding computers within that network to route their Internet traffic through that virtual machine. This would allow the Internet traffic to all go through this encrypted tunnel to the iPredator VPN server, and there that VPN server can go where it needs to go.

So in this example, it would go through to AWS. If you move, in addition to a VPN, you may also want to connect through TOR to further anonymize your IP address. So it could also go through TOR as well before reaching its destination.

Q. If you go from iPredator VPN to AWS, why are there two different pathways depicted in this drawing?

A. There could be several reasons. Either you just want to communicate directly using a VPN without using TOR. One of the disadvantages of TOR is that it's a lot slower because you're traveling through multiple computers.

Other times, too, if you're using TOR and somehow TOR stops working, your real IP address or IP address used may be exposed.

Having a VPN before connecting to TOR is kind of like a fail-safe so that if your TOR connection drops, your VPN can

still establish that connection to the Internet.

Q. So how many layers of anonymity are depicted in -- or represented by Ms. Thompson's computer setup?

A. There are several, at least, you know, two or three. When you are going through a virtual machine, a virtual machine in and of itself is a separate computer. And if you set up a computer for one purpose, for example, just to route Internet through it, your user data that's on your home machine is not present in that virtual machine. This means there's a level of anonymity there because you have a machine that doesn't have any other information on it. You're going through to a VPN server, that's another level of anonymization. And then, of course, you can go through TOR or go directly to just using your VPN service.

Q. And where is the IP address for her home Internet in all of this?

A. That would be on the far left side.

Q. I'm going to move now to talking about the next step that you described, which is the proxy scanner.

MS. MANCA: And, Your Honor, offer Exhibits 109 and 110.

THE COURT: Okay. 109 and 110 are admitted.

(Government Exhibits 109-110 admitted.)

MS. MANCA: Can we display Exhibit 109?

Q. (By Ms. Manca) Can you describe what a proxy is?

A. Yeah. A proxy in its most general term is to -- especially in technology, is to route information through a proxy or a middleman, have that proxy or middleman route that information to the destination, and from there, the destination returns information back to that proxy and then back to the source.

MS. MANCA: Can we do Exhibit 110?

Q. (By Ms. Manca) Okay. And how does what you just described about a proxy relate to a reverse proxy?

A. Yeah. So in this exhibit, for a reverse proxy, this refers to a type of proxy service that is typically used for web applications. A reverse proxy sits at the outermost external-facing part of an internal network. And when a request is sent from an external device to the reverse proxy, it will determine if it needs to grab information from an internal server or resource. It will route that traffic -- it will proxy that traffic to that internal resource, obtain the information that it needs, and then send that back to the external device.

Q. Okay. What's the reverse part?

A. The reverse part is what you see on the right side here; typically, in a forward proxy, it's the other way around. When you are in, for example, a corporate environment and you have internal computers trying to reach out to the Internet, it may route all that traffic through one proxy service. From then, that proxy will forward it to the external recipient.

In the reverse part, this is the other way around, in which

the proxy server is requesting internal resources in order to return data back to the source.

Q. Okay. So that loop on the like right-hand side, that second part of the loop is the reverse?

A. Yes.

Q. Why set up a reverse proxy rather than routing traffic directly from the external device to the internal server?

A. Yeah. There's some good uses for using a reverse proxy, one of them being it hides the internal resource or server, so it essentially protects it from an external-facing device. And it anonymizes so that it's not visible.

Another thing is for performance. Typically, you may hear the term "load balancing." If there are multiple internal servers or resources with the same configuration, the reverse proxy may send the request to one of those services that is not, you know, for example, heavily impacted by a lot of users.

Or let's say if I'm getting requests from U.S., I will route it to a U.S. internal service, if I'm in Europe, to a Europe service, and vice versa.

And secondly, reverse proxy, when it is held in an external-facing server, for example, a web application or web application firewall, it allows, you know, a company or network to kind of filter the incoming requests in order to route them to the appropriate channels or to drop them if they look malicious.

Q. Are you familiar with the term "server-side request forgery" or SSRF?
A. I am, yes.
Q. Is that commonly abbreviated SSRF?
A. It is.
Q. Okay. Can you tell us what that is?
A. Yeah. So an SSRF vulnerability, at its core, is that an external device is using an internally trusted device, typically one that is externally facing, like a web application firewall, and tricking -- essentially tricking that internal device to make an internal request on its behalf that's outside of its intended use.

So in an example where I, an external user, is requesting, for example, information about my driver's license, I will send that to the reverse proxy, and the reverse proxy will grab that internal information, give it -- and send it back to me.

When I'm doing a server-side request forgery, in this example, I may send a request to the reverse proxy, but instead of telling it to grab information about my driver's license, I instead trick it to go ask another server for maybe a list of all the Department of Licensing employees and their addresses and their date of births and send that back to me.

And of course, using this reverse proxy or internal server that is essentially a trusted entity within the internal network, in this case the Department of Licensing, and using

that internal trust to make an action that is not intended -- that it was not intended to do.

Q. Can I show you Exhibit 117?

A. Yeah.

MS. MANCA: And, Your Honor, I offer Exhibit 117 for demonstrative purposes -- I'm sorry, I meant 116.

THE COURT: So 116 is admitted and displayed to you, but for illustrative purposes only.

(Government Exhibit 116 admitted.)

Q. (By Ms. Manca) So can you tell us which parts of this demonstrative depict what you're talking about with an SSRF?

A. Yeah. So starting from the middle to the right where there's a comment that says, I want to do this thing, and then the second part says, okay, you are trusted. What this is doing is it is bypassing and telling the server, you know, regardless of your typical function and your normal course of business, go and talk to this internal metadata service instead and give me information.

Q. How does a SSRF relate to what you've seen on Paige Thompson's computer regarding her hacking activity?

A. Yeah. So I see -- or I saw scanning activities on Ms. Thompson's device where the command that was issued to obtain information from the Instance Metadata Service utilized a form of an SSRF, vulnerability or exploit. She is scanning these web applications, these IP addresses, on AWS environments. And

instead of asking for what it normally would return, she is asking to proxy through this reverse proxy, for example, and ask for information through the Instance Metadata Service, which, you know, according to Amazon and elsewhere, it should be outside of, you know, its intended function.

MS. MANCA: Can we call up -- Your Honor, I'm going to offer as a demonstrative Exhibit 117.

THE COURT: Okay. 117 can be displayed as a demonstrative exhibit only.

(Government Exhibit 117 admitted.)

MS. MANCA: And, Your Honor, I have a blowup of this. May I approach the witness --

THE COURT: Sure.

MS. MANCA: -- and turn that around?

THE COURT: Sure.

This is how we used to try cases, we would draw on the board and have charts. It was so much more fun.

MS. MANCA: I'm seeing now that it's going to be a little small for people, but they also have the screen.

Q. (By Ms. Manca) So we have a version on our screen and then we also have a large blowup

Mr. Ho, can you walk us through the arrows on this drawing? And then we're going to look at some code that relates to this.

A. Yeah. So in the beginning of this at the top left it's looking at the AWS documentation for IP address ranges. What

this means is it's taking a list of all of the IP addresses associated with Amazon Web Services. This is a document that's publicly accessible and available to the public and provided by Amazon.

And what this proxy scanner is doing here is there's a script that will, you know, take the IP addresses. There's approximately 37 million, and it will scan -- it will run those IP addresses through a scanning script. And what this scanning script will do is it will search that IP address, either at a specific port number or elsewhere, and it will identify at the very base level if it can talk to the Instance Metadata Service.

Q. Okay. I'm actually going to stop you there because we're going to unpack that a little bit.

But what you just described, where is that on the demonstrative, is that at the top line?

A. Yes.

Q. Okay. How many IP addresses did Ms. Thompson scan?

A. I'm unsure, but she had access to approximately 37 million.

Q. Where did she find those 37 million IP addresses?

A. They appeared to have been taken from the public-facing Amazon documentation that provides these IP addresses.

Q. So there's a record somewhere of 37 million IP addresses that's publicly available?

A. Yes.

Q. Okay. And what do all those IP addresses have in common?

A. They are all associated with Amazon Web Services.
Q. And when she's doing all this activity, is she using a web browser like Internet Explorer or Google Chrome?
A. No. She's using an application called curl.
Q. And how would you enter the curl command, like what kind of user interface would you use to do that?
A. Typically, this would be used on a command line interface, or CLI. Linux is one of the operating systems that would support using curl.
Q. You used the term "curl," what does curl mean in computer speak?
A. Curl is an application that allows you to make a web request to a specific Internet resource and retrieve information back.
Q. All right. We're coming to -- so we've got the scanner script, and now the arrow comes down and there's the words "grep-metadata," what does that mean?
A. This is another form of script that was identified on Ms. Thompson's computer. But, essentially, grep stands for a tool that is used on Linux operating systems. It's used to search across data specifically like text. And metadata, of course, references data about data.
Q. And what is the scanning script looking for specifically?
A. There's a very specific response that gets returned when you are asking for information from the Instance Metadata

Service on AWS environments. If you're asking solely for just metadata, you'll get a list of responses back. And these responses typically are just categories -- categories of metadata that you would have access to. And the very first one in the metadata response is a keyword that's ami-id.

Q. Okay. And then once she had gathered all of these responses, did she compile them anywhere on her computers?

A. Yeah. She made several places where this information was stored, but there was also a file called mega-metadata.txt.

Q. Okay. We're going to start looking at some of those scripts. We're going to, again, have that physical so we can relate back to that.

MS. MANCA: But can we look at Exhibit 640, please. Okay. Can we blow that up a little bit?

Q. (By Ms. Manca) Okay. Again, not going to run through every line of code, but can you tell me generally what this script does?

A. Yeah. So this -- this is a file called "README." Typically, this is a file that's kind of meant for people to read first or it's kind of like a manual. There's a comment that says "emperical list of ports to scan." But on the third line, what this code is doing is it's taking a .xz file, which is a compressed file, and it is outputting and listing a list of ports for each of the IP addresses, presumably in that file, and running a script to scan and check for metadata responses.

MS. MANCA: Okay. Can we pull up Exhibit 402?

Can we blow up the left-hand corner -- upper left-hand corner?

Q. (By Ms. Manca) Okay. There's -- you've seen this Slack communication before in your work?

A. I have.

Q. It says, Dude, so many people are doing it wrong. I've found loads of EKS clusters exposing 169.254.169.254. Can you explain how this text message relates to your testimony?

A. Yeah. This relates to the proxy scanner that has been mentioned. Essentially, this scan is checking for reverse proxy or server that's exposing 169.254.169.254, which is the internal IP address of the Instance Metadata Service.

MS. MANCA: Can we go to Exhibit 641, please?

Q. (By Ms. Manca) In this script is spool.sh. Can you tell us what this does?

A. In summary, this is taking a range of IP addresses and it is using an application known as Python, which is used primarily for software development, to create a list of IP addresses, and then saves them to a file.

Q. And 642.

So we showed you two exhibits that were related to IP addresses. Where do those relate to the proxy scanner drawing, which is Exhibit 117?

A. The top-half portion.

Q. Okay. Now we're in Exhibit 642. Can you tell us where we are on the drawing over there on the left -- or your right, my left?
A. Yeah. It's going down now from that scanner script to the AWS web-facing servers.
Q. Okay. And once again, it looks like in 642 we're looking at a screenshot of your computer?
A. Yes.
MS. MANCA: Okay. Can we go to the next page of that? And blow that up if we can.
Q. (By Ms. Manca) What is this script looking for?
A. Yeah. So this is one of the scripts that was found on Ms. Thompson's devices. It's looking for specifically the ami-id keyword within a set of folders.
MS. MANCA: And then can we go to the next page of that?
Let's go to Exhibit 643, then.
Q. (By Ms. Manca) So 643 has a number of responses. What are these responses -- what script is generating these responses?
A. I'm unsure which exact script created this file, but what is listed here is a response back from what presumably is metadata from an IP address with the associated port number.
MS. MANCA: Can we go to the next page of this? And the next page.
Okay. And the next page after that.

Q. (By Ms. Manca) What are we seeing here on 643, page 4?
A. So this is the contents of a file called mega_metadata. And this looks like -- it appears to be an output of matched files across folders that are on Paige Thompson's device where it identified a match to the keyword ami-id.
Q. And this is that mega_metadata.txt file?
A. Yes.
Q. So it sounds like if when there's this scanner, there are a number of different types of responses a person can get back in response to the scanner; is that accurate?
A. Yes.
Q. Okay. Can you give us just an overview of what, in general, those responses could be?
A. Yes. So, generally, some of those responses could be -- you know, previous exhibits also showed that there could be an error code like 404, not found. Another one says, you know, forbidden or unauthorized. But when there's a successful return, a response, it will list sort of categories of metadata that you can access, and usually with the first one being ami-id.
Q. So the one she was specifically looking for is this ami-id?
A. Yes.
Q. And when she gets that back, what does that mean? What does that signify?
A. That means -- so this is like one of the first steps. This

means that she can successfully talk to the Instance Metadata Service externally using the IP address that was listed in that file name.

Q. Okay. And once she got these responses back, these successful responses of ami-id, where did she put them?

A. She would store them in files like this or within that AWS hacking directory.

MS. MANCA: Let's go to Exhibit 644.

Q. (By Ms. Manca) Do you recognize this?

A. Yes.

Q. Okay. Can you tell us what this is?

A. Yeah. This is a separate type of scan which is now looking for information about the IAM Role associated with the IP address that's listed in these commands. So whereas the previous command looked for just the list of potential metadata to ask for, this command is specifically asking for information about the IAM Role. Typically, the IAM Role is the one that is assigned to that server that's being exploited, the reverse proxy.

Q. Okay. So we've moved to the next step now.

A. Yes.

Q. As we're moving from step to step, is that a manual process or is that automated?

A. So that would be a manual process.

MS. MANCA: Okay. Your Honor, I want to offer

Exhibits 118 and 119 for demonstrative purposes.

THE COURT: Okay. 118 and 119 can be displayed to the jury as demonstrative exhibits.

(Government Exhibits 118-119 admitted.)

MS. MANCA: Can you pull up 118?

Q. (By Ms. Manca) Does this exhibit describe the process of obtaining information like you were just describing in that last exhibit?

A. Yes.

MS. MANCA: Okay. Your Honor, may I approach and put up a blowup of this as well?

THE COURT: Sure.

MS. MANCA: We may not need it.

Q. (By Ms. Manca) Okay. Can you walk us through what's happening in this drawing from left to right?

A. Yes. So this is representing the curl command that is used to obtain information from the internal metadata service. So there is a request, a curl request, that is issued by the external device. And it is querying information to get back the metadata information.

MS. MANCA: Okay. Can we go back to Exhibit 644?

Q. (By Ms. Manca) This highlighted portion of this response, can you tell us who this relates to? Do you know what company this is?

A. That would be a company called 42Lines.

Q. And what information has been received about 42Lines in response to this curl command?
A. This information provides the IAM name, the role name, once the command was asking for the IAM information.
MS. MANCA: Can we go to 645?
Q. (By Ms. Manca) Okay. And there's a highlighted role, what role is that?
A. EC2 read only.
Q. Do you know what company used that IAM Role?
A. I don't recall at this moment.
MS. MANCA: And can we go to Exhibit 646?
Can we highlight that highlighted one?
Q. (By Ms. Manca) Do you know what company used that role?
A. Yes. This one was for Capital One.
MS. MANCA: And Exhibit 647.
Q. (By Ms. Manca) Do you know who uses that role?
MR. KLEIN: Your Honor, do you mind if we just slow down so we can look at these?
THE COURT: Slow down?
MR. KLEIN: Yes. I was just trying to absorb that information.
THE COURT: Okay.
Are you ready?
MR. KLEIN: Yes, Your Honor.
THE COURT: Okay. Got it.

Q. (By Ms. Manca) Do you recall which company used that role?
A. I'm unsure.
MS. MANCA: Okay. We'll go next to Exhibit 457, the second page.
This is an IRC chat. There's a reference here to EC2 user data with 169.254.169.254 in the first line. And then a few lines later people setting up proxies on EC2 and not filtering access to 169.254.169.254. Can you explain what this means and how it relates to your testimony?
A. Yeah. This is essentially talking about the vulnerability, the fact that the instance or internal metadata service is essentially exposed to the open Internet that would allow an external user to query access to that service.
Q. I'm going to move now.
What is the next step after obtaining the metadata IAM Role?
A. Yeah. So once you have the name of the IAM Role, you can use that name to query the Instance Metadata Service again for security credentials related to that role. So in order to obtain security credentials for one of these IAM Role accounts, you need to know the name in order to obtain that.
Q. Is this next move from metadata info to IAM credential manual or automated?
A. It's typically manual.
MS. MANCA: And can we pull up Exhibit 119?

Q. (By Ms. Manca) What are we seeing in Exhibit 119?
A. So this is obtaining the IAM Role information once, you know, a user has obtained the metadata information. So that part where -- in the file -- for example, that mega_metadata file where you see an IP address at this port has the exposure for that ami-id term, which lets you know that that server is vulnerable and exploitable because you can talk directly to that Instance Metadata Service.

Once you have that information, you use further information to ask for the name of the IAM Role, and that is what's occurring here.

MS. MANCA: Okay. And, Your Honor, I'd like to offer Exhibit 120 for demonstrative purposes.

THE COURT: 120 may be displayed to the jury.

(Government Exhibit 120 admitted.)

Q. (By Ms. Manca) Is this the next step after a -- Ms. Thompson had the IAM Role information?
A. Yes.

MS. MANCA: Okay. And, Your Honor, may I show a demonstrative of that?

THE COURT: Oh, sure.

MS. MANCA: I'm going to switch screens.

THE COURT: Yeah.

Q. (By Ms. Manca) Okay. Once again, can you walk us from left to right on this demonstrative?

A. So once you have the name of the IAM Role, what you're going to do now is essentially request information, the security credentials of that role, and then authenticate as that role using an application known as AWS CLI, or command line interface, which was previously mentioned before.

This is separate from, you know, directly talking to the vulnerable or exploited proxy server and getting that information. This part is now a different entry point into the AWS or Amazon environment. The AWS CLI provides the ability to run, you know, Amazon-specific commands in like a management interface. So, essentially, it's like a control panel for your AWS environments.

Once you have that IAM Role information, you would request the security credentials from that Instance Metadata Service, take that credentials, and then separately authenticate using the AWS CLI. And now, once you're connected, you can run additional commands such as, you know, ListBuckets or, you know, GetObject, or sync.

Q. What factors -- you know, once Ms. Thompson authenticated in to the AWS CLI, or command line interface, what factors determined what powers or permissions she had within that environment?

A. Yeah. So that would have to be the role permissions that are assigned to that specific IAM Role.

MS. MANCA: Can we call up Exhibit 670?

Q. (By Ms. Manca) So Exhibit 670 is a screenshot of your forensic tool; is that right?
A. Yes.
MS. MANCA: Okay. Can we go to the second page of that document?
Q. (By Ms. Manca) And this is the actual script that was shown in your screenshot?
A. Yes.
Q. Okay. What is the name of this script?
A. It's a-q-u-i-r-e, which I believe is meant to spell acquire, underscore, aws_info.sh.
Q. And where was this script located?
A. This was located in that aws_hacking_shit directory.
Q. We've seen .sh a lot. What does .sh mean in computer language.
A. .sh is a file type that is typically used as a shell script. So this allows this file to be run on, for example, a Linux command line, so it's a -- yeah.
Q. Someone described it to me once, you hit enter and it goes "bloop." Is that kind of what it is?
A. Yes.
THE COURT: Did you get that, my court reporter?
THE COURT REPORTER: (Nodded affirmatively.)
THE COURT: Good. Yeah.
You know, I once did a case involving ZZ Top and Chrysler

Corporation. Shows you how much fun that was. And this is way back in the early 2000s when you still had the big auto shows. And they wanted to use one of ZZ Top's songs to roll out the Plymouth Prowler at the car show. And ZZ Top said, you can't just rent one of our songs, you have to buy our entire book of songs. And it cost like 14 million. And they were like, that's okay. But they used it anyway, and they just didn't pay or do anything.

So part of the defense of Chrysler Corporation was, well, this particular song from ZZ Top was actually stolen from Norman Greenbaum's Spirit in the Sky, and stolen from John Lee Hooker's song.

So I'm on the bench and I'm saying to the lawyers, no, no, Spirit in the Sky goes, da-da-da-da-da-da-da-de-da-da. And the ZZ Top song goes, da-da-da-da-da. And, you know, she looks up at me like, Judge, what do you expect me to do with that? Just like my court reporter will now.

But, anyway, we'll go back to basics.

MS. MANCA: Thank you, Your Honor.

Q. (By Ms. Manca) So there are a bunch of green hashtags in these -- this script. What -- what are those hashtags?

A. So these are commonly referred to as comments. Typically, in software developments, a user may comment parts of their programming code.

A comment is just essentially a note. There's no parts of

that line that is commented or in green, are not run as part of the script. It's kind of a way for software developers typically to comment and, you know, make notes about what their code is doing.

Q. So the first hashtag is "how to use," and it has that grep ami-id. What is this script doing, this part of the script?

A. So this part kind of provides you information on how to run the script, how to go through the process of, you know, connecting to a compromised or exposed host with their ID address as well as the IAM Role name, and then use that to insert into the script and execute it.

Q. And what about the -- there's an "export regions." Do you know what that export regions part of the script does?

A. Could you show it up?

Q. Yeah, 670 at page 2.

A. So this section of the code is defining, you know, these names here for regions. And these regions correspond to Amazon or AWS regions.

MS. MANCA: Okay. And if we could go to the next hashtag, which is "grab user-data," have we seen that script before?

A. Not during the previous exhibits, no.

Q. Okay. So this is different from even the other scripts we had seen.

What is the function of this script?

A. So this script is similar to the metadata script, except as you see on the right-hand side, instead of asking for metadata, it's asking for user data.
Q. What's the user data that's getting grabbed here?
A. It depends on what's available at that resource, but it would be, you know, user-specific data, as the name suggests.
Q. Okay. Would it include the IAM Role name, or something else?
A. Sometimes, yes.
MS. MANCA: Okay. Can we go to the next one?
Q. (By Ms. Manca) This is hashtag, "get security credentials." What is this doing?
A. So this is -- this script, to summarize, is taking the IAM Role name that is provided when the script is ran or executed. And it is using that curl command to get the security credentials of that IAM Role. Once it has that information, it is then at the very bottom where you see where it starts with "eval," it is sending that content to a script called awssession.sh.
Q. Okay. We're going to get to awssession.sh in just a moment, but I want to ask you about that line above that ends with iam/security-credentials/, and then there's a dollar sign and a 2. What is the $(2) doing?
A. Yeah. So the dollar sign and the 2 in the brackets, what this denotes in a script. Especially when you're executing it,

it denotes what are called arguments. So if you look at the top of the commands and in the comments of the script, there are two arguments that this script takes.

An argument means an input of user data, so the manual inserted piece of information that you put with the script. The first one, the $(1), would be the IP address, that is the exposed or vulnerable service. And the $(2) would be the name of the IAM Role, so one that has already been taken from the iam/info in the Instance Metadata Service.

Q. Okay. And we are going to talk about awssession.sh, but can you give us a preview of what that script does?

A. Yeah. The script will take the data that is returned from the security credentials from the Instance Metadata Service and extract out the key -- the secret key and the token, all of which are required to authenticate, onto the IAM Role name.

Q. Okay. And then returning to Exhibit 120, which is blown up to your right, is this happening at the AWS CLI?

A. So the get security credentials part, the first half, is not. The second half for the awssession.sh is happening at the AWS CLI level, yes.

MS. MANCA: Okay. Let's go to some of the next....

So there are a number of functions here. Can we highlight from "log get-caller-identity" to "try create keypair"?

Q. (By Ms. Manca) Okay. We're going to run through these functions, try to just do it at a high level.

So what is "get-caller-identity" trying to do?

A. So it's trying to get information about, you know, as it suggests, the caller identity for that Amazon environment.

Did you want me to go through the whole thing?

Q. Yeah. Let's do the ones that you described as reconnaissance activity earlier in your testimony.

A. Yeah. So it would be the -- you know, around the first four commands that you see with the four comments, so the "get-caller-identity," the EC2 instances, the S3 buckets, and the security groups. All these commands essentially are asking for information about environment that it's currently connected to.

Q. Okay. How do security groups relate to operation in a AWS environment?

A. So the security groups provide the ability to set certain role -- or not role, but security permissions for either an instance or for a user or an IAM Role.

Q. And then we have down there hashtag "random key id," and hashtag "try create keypair." What's the significance of these scripts?

A. So these scripts is to generate kind of a key ID to use to generate a key pair onto the AWS environment. What this means is, you know, as I mentioned before, to create a key pair of a public and private key, which would be used to have an additional access onto a system.

Q. And we went earlier in your testimony to an exhibit called 608, which was AWS commands. If we were to go back there now, which we're not going to do, would we see evidence of these kind of commands being run by Ms. Thompson?

A. Yes.

MS. MANCA: I'm going to go to Exhibit 671.

And can we do page 2 of that exhibit?

Q. (By Ms. Manca) So -- and I can't remember if I asked you this, this aquire_aws_info 670 that we were just looking at, Exhibit 670, where in the file directory was that?

A. That was in the aws_hacking_shit directory.

Q. Okay. Now, awssessions is somewhere different. Where is awssessions.sh?

A. This one is in the AWS scanner directory.

Q. Okay. And this is, once again, on page 2 of Exhibit 671, a screenshot of your forensic tool?

A. Yes.

MS. MANCA: Okay. Can we go to page 3 of that exhibit?

And highlight the top portion, please.

Thank you.

Q. (By Ms. Manca) So what is awssessions.sh doing?

A. It is taking the content that was provided by the security credentials once it's accessed from the Instance Metadata Service, and it is taking that piece of data and extracting

three things, the access key, the secret access key, and the token. And then it is setting that at the bottom here of the screen as these variables known, like the aws_secret_access_key, and et cetera. What this is doing is it's setting these parameters with the three that it took from the security credentials data and essentially setting the AWS CLI command to authenticate as that.

MS. MANCA: Can we look at Exhibit 672?

Q. (By Ms. Manca) This is a file labeled "credentials." Where did you find this on Ms. Thompson's computer?

A. So this file was located in the .aws folder that is located in the Erratic user directory.

Q. And do you recognize what this file contains?

A. Yes.

Q. What is it?

A. So the AWS command line application has the ability to save access keys and secret access keys that you have used, also known as credentials, by Amazon documentation. And what you're seeing here is access keys that were used by the AWS CLI application to authenticate the names that are put in the brackets can either refer to a number of things, but they could be user generated or named by the user.

MS. MANCA: Okay. And could we go to Exhibit 673? And page 2 of that exhibit.

And page 3.

Q. (By Ms. Manca) Okay. What is the significance of Exhibit 673?

A. This is an example of what would be returned when you are requesting security credentials from, you know, an IAM Role that you are asking from the Instance Metadata Service.

MS. MANCA: Can we go to Exhibit 675?

Q. (By Ms. Manca) What are we seeing in this file labeled "aws.commands.txt"?

A. So in that line, the one that's highlighted appears to proxy through an IP address that has been identified as a Capital One IP address, request security credentials, or the ISRM-WAF-Role, and push that response to the awssession.sh script.

Q. And then is this an excerpt from Exhibit 608, the larger file of AWS commands?

A. Yes.

Q. There's also in the middle "aws s3api sync." This is line 4644, 4645, 4646. What is the significance of that series of commands?

A. You know, as it was mentioned earlier, the sync command is essentially to download data from an S3 environment. Other significance of the command show that these series of commands were run, it's a session, but also, since there were parts where it has, you know, dash, dash, help, or help, it shows that these series of commands are indicative of manual entry, as opposed to

automatic entry.

MS. MANCA: And then if we could -- Agent, if you could pull out and highlight 4719. Actually, 4711 and 4719.

Q. (By Ms. Manca) What is the significance of these two commands?

A. So 4711 is similar to the command I explained earlier about taking the ISRM-WAF-Role and authenticating to that.

The second line is essentially the command we've seen before where the command line interface is asking to list all of the buckets, create a folder name ISRM-WAF-Role, and call up the contents into that folder.

Q. Where have we seen that command before outside of Ms. Thompson's computer?

A. The April 21 gist file.

Q. Okay. That's Exhibit 204?

A. I believe so.

MS. MANCA: Can we go to Exhibit 676?

Q. (By Ms. Manca) This is a file labeled "notes 2." Do you know where this is from?

A. Yes. This was identified on Paige Thompson's laptop device 1b2.

Q. And there's a highlighted session at the top. What is the significance of that highlighted portion?

A. So this highlights kind of the same command to authenticate for a specific IAM Role, the unicredit-prod-logging. Unicredit

has also been referenced in the aws_dumps folder. And then there is on line 56 kind of a response that is sent back to that command, or is indicative of being a response sent back to that command.

MS. MANCA: Okay. Can we pull out of that?

There's some other comments here. Can we highlight the bottom third of these notes?

Q. (By Ms. Manca) What are the comments on these notes?

A. There's one that says "well then..." Further down in the middle it says "Another unfixed previously used account."

MS. MANCA: And then can we go to Exhibit 677?

Can we highlight the bottom third.

Q. (By Ms. Manca) So this file is -- "notes" is the label of it. Where was this notes file?

A. This was also found in Paige Thompson's laptop device 1b2.

Q. Okay. And there are a couple of comments here or, actually, three comments. Can you read those comments?

A. Yeah. The first one is "ec2 read access and s3api read." The second one is "guess whos back." And the last one is "apperian ec2 readonly/s3api limited."

Q. Okay. Does Apperian one of the companies that was shown up in that aws_dumps folder [sic]?

A. Yes.

MS. MANCA: Can we go to Exhibit 455, the third page?

Q. (By Ms. Manca) Do you recognize this as a chat log from

Ms. Thompson's computer?
A. Yes.
Q. Okay. Can you describe to us what's happening in this chat?
A. So the first half is Ms. Thompson showing some commands that she sent or used or executed. And then, you know, there's some responses back from those commands that she appears to send as well.
At the last half of the chat where she is asking if anybody wants a domain or storage gateway or a db.r4.large dump, those reference that she's talking about the vulnerable or exploited server that has this type of information or this type of access.
Q. And her comment is "heh, heh, heh, gottem"?
A. Yeah, as it appears there, yeah.
Q. We're going to move now to the conversation of data theft, okay, so we're moving into the next phase.
If we are talking about data from companies, where are we in this chart 120 related to permissions?
A. So those would be permissions that would allow access to the S3 portion within that diagram.
MS. MANCA: Can we show Exhibit 605, please?
Q. (By Ms. Manca) Okay. You previously testified that this is the folder aws_dumps?
A. Yes.
Q. Okay. There -- the files in here have a -- I don't know if

you'd call it a suffix, or whatever you call it on the end, .tar.xz?

A. Yes.

Q. What you do you call that thing on the end?

A. So it's the file extension.

Q. So the file extension is tar.xz. What does that mean?

A. So the tar part is short for tarball. It's a compressed file format, similar to like a .zip file. And the .tar just shows that it's an archive file with a lot of files or folders inside of it potentially.

The .xz part stands for another compression algorithm that's used to kind of shorten the size of the data. It's to kind of compress it further than a tarball already is.

The .xz is a known compression format that's considered a lossless data format, which means that this type of compression algorithm is designed to ensure the contents of the data is in its original state and has, you know, the original data within it.

Q. Okay. What are some of the reasons that someone would compress a large amount of data?

A. There's several reasons. One is, you know, if you have a large number of files, they'll take up a large number of storage space, you may want to zip it all into one file to reduce space.

Second, if you're copying the file from, you know, one drive to another, transferring one file is much faster and

easier than transferring, say, 10 million files.

Q. Okay. Do you have evidence on Ms. Thompson's device that these files were moved from one place to another?

A. Yes.

Q. Okay. Can you tell us what that evidence is?

A. So there are forensic artifacts on two parts of Ms. Thompson's devices. The two large RAID arrays or storage devices, as I mentioned earlier, one was approximately 6 terabytes and one was approximately 11 terabytes. One of the drives, MD127, appeared to contain forensic evidence that these files existed on that drive at some point.

These current files in its iteration was found on MD126 under that aws_dumps folder.

So there's forensic evidence that suggests that the data was copied from one drive to another.

Q. Is there forensic evidence regarding the date that that move would have happened?

A. Yes. So it would have occurred sometime in the, I think, approximately the June or July time frame.

Q. And are you basing that on -- or can you tell us based on this exhibit what you're referring to?

A. So this part would have been the modified date. This would be when essentially the file content was modified or created. I -- I don't think I would be able to tell from this exhibit when they were copied over.

Q. And so there are dates running down the middle of this file directory. What -- what do those dates mean?

A. So those dates mean in this context the modified date. So this is the date that said file was created.

Typically, you have several timestamps, you have a creation date and a modified date, and also an access date for our file.

If the file was, you know, created on a hard drive and then modified at a later date, the creation date may come before the modified date. You know, you created a file today and then I, you know, used it and saved it tomorrow, I would have a modified date of a later time.

However, if you look at forensic evidence, if there's a set of files that have a modified date of March, for example, but they have a creation date of July, initially it sounds a little off that the creation date is later than the modified date, but what that just means is that when a file is copied over to another drive, that file that gets copied over has a new creation date because those files were transferred and created there. However, the data hasn't changed, it hasn't been modified since March, so that timestamp still stays within that device as well.

Q. Okay. So I'm showing you another version of this file directory at 701. Can you tell us what additional information is here that informs your analysis?

A. Yeah. So as I mentioned earlier, you see on the modified

date and timestamp there are dates around the June -- the late June 2019 time frame. And then you have a created date that all show July 12th, 2019. This is indicative of a file or these sets of files being copied over to this drive on July 12th, 2019.

MS. MANCA: Can we go to Exhibit 711?

Q. (By Ms. Manca) Do you recognize Exhibit 711?

A. I do.

Q. Can you tell us again, based on your analysis of the computer and this file directory, what date these files were downloaded?

A. It appears to be around the March 2019 time frame.

Q. Okay. And you say, "it appears," why do you say that?

A. So there's -- there's some entries here, for example, in May. If user, in this case Ms. Thompson, would have changed some of the files, the modified date may look different.

Q. I see. Okay.

So if there are instances here where we see a May date or a June date or some other date than March 22nd, then that's indicative of that file having been modified after it was downloaded?

A. Could be, yes.

Q. Okay. Would it be changed even if someone just looked at it and didn't do anything with it?

A. No.

THE COURT: Is this a good place to take the afternoon break?

MS. MANCA: I think so. Thank you.

THE COURT: Okay. It's pretty heavy sledding here, so, yeah, we'll take our break now.

And please go down to the 14th floor, and we'll have you back on -- in your seats at 3:00.

THE FOLLOWING PROCEEDINGS WERE HELD OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: So, Mr. Klein, I was very worried yesterday that with all that rain Ms. Meister was going to flee. Did she head south or?

MR. KLEIN: Your Honor, she did flee because of the rain.

THE COURT: Yeah.

MR. KLEIN: And I was thinking of it, too, but...

THE COURT: But you're in need of --

MR. KLEIN: Yeah. I went to high school and college here, yes, so I'm used to it.

I did bring an umbrella this time, which everyone called me out for already.

THE COURT: No. You're allowed to use an umbrella on a day like yesterday. That was a horrible day.

MR. KLEIN: Ms. Meister will be back, I believe, Tuesday morning.

THE COURT: Okay.

MR. KLEIN: She had some childcare issues.

THE COURT: No problem. I was just wondering if she -- okay, so let me --

You can step down. Sorry, Mr. Ho.

In regard to what I'm going to allow in regard to Agent Henderson and Mr. Strand, you know, I will allow each of them to testify in their general area: Agent Henderson about credit card fraud and the ability to sell things on the dark web and those kinds of things. I will not allow him to give an opinion or to state that what Ms. Thompson did shows she was going to -- she was trying to do that or anything like that.

And then in regard to Mr. Strand, likewise, I will allow him to talk in general about white hat hacker, grey hat hacker, black hat hacker, and the general hacking community standards for if you see something, how do you say something, but not to say that what Ms. Thompson here did means she's a black hat hacker or she had intent to defraud or criminal intent or anything like that. So general expert testimony about the subject matter, yes; applying that to this case, no.

Do you need any clarification, Mr. Friedman?

MR. FRIEDMAN: I do have two questions.

THE COURT: Okay.

MR. FRIEDMAN: One with respect -- with respect to Special Agent Henderson, one of the areas of his testimony was

going to be about value of the data.

THE COURT: He's allowed to testify that this type of information would be worth more than $5,000 to people who knew how to monetize it and use it, yeah.

MR. FRIEDMAN: Okay. And I'm assuming the Court's ruling doesn't mean that he can't look at certain like documents that says carding forums dark web and say what is a carding forum dark web.

THE COURT: He's allowed to testify about those things, yes.

MR. FRIEDMAN: Okay. Thank you.

THE COURT: And.

MR. HAMOUDI: Your Honor, I think my concern is they're web searches; right?

I would understand if we had a situation in a case where there was actual -- there was actual carding like contraband and he would look at them, is this consistent with what you would see with web searches. There's no evidence that anything was even downloaded, so that's my concern is that --

THE COURT: Yeah. And you've made that point already, and you'll make that point in cross-examination of him that, you know, people look at the Internet. We're not -- we don't punish people for doing Google searches or web searches, do we? No, we don't. And there's no evidence that you've seen that anything like that was done in this case. Be careful on that one. But,

yeah, you know, I understand that there's a risk here for the defense, but I do think the clarification for the jury is something I want to do. These are a lot of tough concepts. I'll grant you everyone kind of understands identity theft in the sense that their -- that juror we had who talked about, I'm so tired of this, I get these notes all the time, but they don't know about the dark web, they don't know about how these things are utilized by people in, you know, Romania or other parts of the world and stuff like that. So I think a little expert testimony in that area will be allowed, okay?

MR. HAMOUDI: I understand, Your Honor. Thank you.

THE COURT: Mr. Klein?

MR. KLEIN: Just a clarification on Strand, Your Honor. The government had indicated they wanted him to testify to like various ethnical codes. And my concern is, Your Honor, there's no evidence Ms. Thompson ever agreed to any of these, and it's going to make it sound like she did or that she's somehow bound by them and these are completely voluntary things.

THE COURT: Yeah. We'll make that very clear that there is no -- these are not laws or government regulations. But, you know, I think that just an understanding of what the hacker community -- you know, the kind of things that Kat Valentine was talking about, will be allowed.

MR. KLEIN: And then I assume since that is coming in that our expert, Professor Halderman, who's here, can testify

about those same areas, too, in response.

THE COURT: You assume correctly.

Okay. So let's take our break. And at 3:00, we'll start again, so be here.

And at 4:00 or so when we quit, we'll give you some draft instructions.

Now, these are draft instructions done by my law clerk, Laura Daugherty. I haven't blessed them yet, but they're good for you to look at and respond to on Monday, okay?

MR. HAMOUDI: Your Honor, there's a matter that I need to take up outside the presence of the government, and I don't know when is the best time.

THE COURT: I'm sorry, outside the presence of the government?

MR. HAMOUDI: Yes, Your Honor.

THE COURT: How about -- hmm, I'm going to the Mariners game, so like 6:00?

No, I'm just teasing you.

We'll do it at 4:00. When we send the jury away, we'll send the government away.

MR. HAMOUDI: I appreciate that, Your Honor. Thank you.

THE COURT: Okay. And of course you're all wondering what happened with the ZZ Top case. I let it go forward and they ended up settling for about $3 million.

Now, remember, Chrysler had a prior. They went to Bruce Springsteen in the '80s and said we want to use Born in the U.S.A., and he said no. And so they changed it to Born in America, which I think was tacky. And he never sued or anything like that, but they settled for about 3 million bucks.

Thanks.

(Court in recess 2:46 p.m. to 3:04 p.m.)

THE FOLLOWING PROCEEDINGS WERE HELD
IN THE PRESENCE OF THE JURY:

THE COURT: Go ahead, Ms. Manca. You may continue. How much more do you think you have for Mr. Ho?

MS. MANCA: I definitely have another hour.

THE COURT: Okay. And that hour is 3:00 to 4:00? Yeah.

MS. MANCA: I'll keep motoring through.

Q. (By Ms. Manca) Mr. Ho, you heard Mike Fisk testify about the Capital One data that he was provided by the FBI to review and that he identified as Capital One data?

A. Yes.

Q. That was 712 and 713, for the record.

Did you pull those exhibits to be provided for Capital One's review?

A. Do you have that?

Q. Yeah.

MS. MANCA: Can we pull up Exhibit 712? Okay. That

one. And the next page. And Exhibit 713.
Q. (By Ms. Manca) Do you recognize these documents?
A. Yes.
Q. And you actually pulled those from Ms. Thompson's device?
A. I did, yes.
MS. MANCA: Can we show Exhibit 720?
Q. (By Ms. Manca) Where was this file directory located?
A. There was within the Apperian folder. This would have been from the tar.xz file that was named Apperian.
Q. Can you tell from this file directory and other information on the computer when these files were downloaded?
A. Yeah. So once the tar.xz was extracted, the files here appear to show a March 7 to March 8 time frame.
Q. And you had mentioned an extraction, so we were talking about those files had that extension tar.xz. Is there a process to get to this file tree we're looking at right now?
A. Yeah. There's an application that you can use to extract the data from those files.
Q. Okay. So what we're looking at right now is the extracted version?
A. Yes.
Q. And you said, based on this information, you can tell when the files were downloaded?
A. Yes, approximately.
Q. And what is that approximate date?

A. March 7 through March 8 of 2019.

MS. MANCA: Can we pull up Exhibit 730?

Q. (By Ms. Manca) Is this also an extracted file from aws_dumps?

A. Yes.

Q. And approximately when were these files downloaded?

A. Around March 28th, 2019.

MS. MANCA: And can we pull up Exhibit 740?

Q. (By Ms. Manca) Is this another extracted file from aws_dumps?

A. It is.

Q. And approximately when were these files downloaded?

A. So it varies, but the oldest date appears to be March 12th of 2019.

Q. And, finally, Exhibit 750. Is this another file from the aws_dumps folder?

A. Yes.

Q. And approximately what date were these files downloaded?

A. Around March 5th, 2019.

Q. I want to draw your attention to Exhibit 780. Do you recognize these commands?

A. Yes.

Q. Who are they from?

A. It's from the AWS commands file.

Q. What do these commands do?

A. So the first two are using the application grep, which I mentioned earlier is to search. There are some additional options with the grep, the dash Ri, which "R" means for "recursive," so it's telling this application to search across all of the files and directories and subdirectories, "i," which means "ignore case," so whether it's upper case or lower case, and it's searching for the term "Seattle."

The first command appears to be an error, which is fixed on the second line. The dot indicates to search its current directory of where it's at. And then the greater-than sign then goes to this file called Capital One inclusion list, to be saved in a folder called aws_scan.

Q. Did you find a folder titled Capital One inclusion list in the aws_scan folder?

A. I found a filed called Capital One inclusion list.

Q. Where was that file when you found it?

A. I believe it was in the aws_scan folder.

MS. MANCA: Can we look at Exhibit 781?

Q. (By Ms. Manca) Do you recognize Exhibit 781?

A. Yes.

Q. And once again, we're looking at screenshot of your forensic tool?

A. Yes, that's correct.

Q. And it's really tiny print, but can you see where the file --

MS. MANCA: Actually, can we back out of that and show the file directory, the file pack?

Q. (By Ms. Manca) Does that refresh your memory in the blurry text about where this was located?

A. Yes. It was identified in that aws_scan folder.

Q. Okay. And that was located in which larger folder?

A. The aws_hacking_shit folder.

MS. MANCA: Okay. Can we pull out of that? And now can we highlight the bottom half?

Q. (By Ms. Manca) So what is the Capital One inclusion list?

A. So the Capital One inclusion list appear to be the output of using that command grep, which we had seen earlier. What that program is doing is searching for the term "Seattle" across the data set at the current directory. The directory of where it is unknown, based off of the commands. But what it's matching here is several files.

So if you look at each of the lines, you'll see, for example, the Acxiom-inclusion-list, slash, and then the following file, it is indicating there is a match for the keyword "Seattle" in this file, and it continues on with each line in this Capital One inclusion list file.

Further analysis identified that the files that it was searching that had this inclusion list are related to files that were taken from Capital One.

Q. And there's redactions here. Do you know what information

was redacted?
A. Yes. So it appears to be email addresses, as well as it looks like physical address information.
Q. And is the actual data on the computer redacted?
A. No.
MS. MANCA: Can we go to the second page of this? And pull out of the magnification.
Q. (By Ms. Manca) Do you recognize this second page as a full copy of the file -- not the full copy but --
A. Yeah, it's a portion of the --
Q. -- portion?
A. Yes.
Q. Okay.
MS. MANCA: Agent Martini, can we scroll through the entire exhibit? Page 3, page 4, page 5, page 6, page 7, page 8, page 9, page 10, page 11, 12, 13, 14.
Q. (By Ms. Manca) So this file was PDFed. How -- when you pull it up on your screen and you're looking at it, sitting in your office, what does it look like?
A. It's a line of text. So it goes really, really, really wide. So I could see, in the PDF, where the pages are kind of expanding to the right. So each of the lines in this file represents, you know, the location of where the Seattle keyword was found, plus a very long line of text that goes horizontally.
MS. MANCA: Can we go to page 5 of that exhibit?

Q. (By Ms. Manca) Do you know why the formatting is different on the top two lines versus the, you know, remaining 80 percent of that file?
A. Yeah. So these are from two separate files where the keyword Seattle matched.
Q. What does that mean about the way these files were stored in the Capital One database?
A. It means that the data was stored at multiple locations.
Q. And then it gets all pulled and compiled into this list?
A. Yes. The grep application is searching through all those files for those matches.
Q. And up at the top, there's date of birth and the last four SSN redacted. Those redactions are for court, but what is the unredacted portion of that exhibit?
A. That would be the actual content of -- you know, for example, the full date of birth and the last four of the Social Security number.
Q. Okay. And then these really big blocks of text right before "Seattle," what is redacted from that?
A. Those would be, you know, typically, the physical mailing address.
Q. And what do all the people on this list have in common?
A. There's a reference to Seattle either through the city that's located, or also maybe an email address or something that would have the keyword Seattle.

MS. MANCA: Can we go back to the first page of this exhibit?

Q. (By Ms. Manca) Can you tell, based on the information you had in your forensic image, when this list was created?

A. It would be created sometime on March 28th, 2019.

Q. And then is there any evidence that this list was moved or archived or stored?

A. Yeah. So as I mentioned earlier, the creation date has a later date of July 10th, 2019.

Q. What does that later date of July 10th, 2019, indicate?

A. The file had been copied from one location to another.

MS. MANCA: Can we look at Exhibit 782?

Q. (By Ms. Manca) And, actually, it looks like we're still in this aws_hacking_shit aws_scan folder; is that right?

A. Yes.

Q. And there's another file identified as "ID." What is that?

A. This file contains some text that appears to be related to an individual named Joseph Baleda.

Q. And where is this information coming from?

A. So if you look at the top of the one here, it appears to be coming from this file that's in that, you know, abbreviated pre-approved email -- EML offers processed, all the way up and to that file ending in ts-inclusion.json.

Q. And is Joseph Baleda's information included in the Capital One inclusion list?

A. Yes.
Q. Based on the information in the forensic image, can you tell when the ID was created?
A. It also appeared to have been created on March 28, 2019.
Q. And can you tell whether this file was also stored or modified in some way after it was created on March 28th, 2019?
A. Yes. It had a creation date of July 10th, 2019.
MS. MANCA: Can we go to Exhibit 457, page 4?
Q. (By Ms. Manca) This is a lot of text, and we're not going to through all of this, but have you had a chance to review this prior to your testimony today?
A. I have.
Q. And based on what you read, what are these conversations or messages talking about? Just subject matter.
A. It's talking about ways to store or kind of move around data in a more accessible manner.
MS. MANCA: And can we go to Exhibit 458? And page 2 of that. If we could highlight that bottom part.
Q. (By Ms. Manca) What was the significance of this IRC chat, and specifically the reference to snappy-parquet?
A. This references parquet, which is a type of file format that's used or created by the Apache Corporation. So this type of file, a parquet, is typically used with data processing applications, typically those that are generally known as, you know, big data processing applications.

And then the other significance is that part of the name on the second line, the second message, the mentioning of the buckets asvsbclinemanagement-us-east-1 is also a bucket that was identified as Capital One's data.

Q. So we're going to switch gears and leave data -- well, we're also going to stay with data, but we're going to go to Exhibit 602, page 5.

Do you recognize this as part of the file tree for aws_hacking_shit?

A. I do.

Q. And right in the middle, there is a reference to a folder called "miner." Do you recognize that?

A. Yes.

Q. What do the files in this folder relate to?

A. They relate to applications or scripts that would be used to deploy a cryptocurrency miner. It also relates to the usage of a docker container.

Q. And we'll talk about dockers, but can you tell when this mining script was last modified?

A. So the folder itself was last modified around June 15, 2019, but that would most likely be from the tmp file with that modified date. The earliest I see is March 8 of 2019. But outside of the June time frame, the latest would be March 22nd of 2019.

Q. And we're going to run through these scripts, but which of

these on the list is the one that is the complete miner script?
A. It would be the third file in that folder, the minersetup_eth.sh.
Q. Okay. Let's start with Exhibit 800. What is this docker file script?
A. So the docker file is sort of like a configuration file that's used to create something called a "docker container." Similar to how I mentioned a virtual machine is its own separate operating system, a docker container is a subset of that. It is a virtualized contained space that allows you to run applications within that virtual space. So it's kind of like a -- it's a portion of a virtual machine, if you will, that will allow you to run code.
Q. Okay. Can we go to Exhibit 801?
Is this also related to Ms. Thompson's mining script?
A. Yes.
Q. Looking at the top, it says "export eth_account," and then a long series of numbers and letters. What is that long series of numbers and letters?
A. So that would be the Ethereum account in which the cryptocurrency miner would report the funds to.
Q. Is that also referred to as a "wallet," or something different?
A. It would be part of a wallet, but it would be the public key address for Ethereum.

Q. And then there's placement curl command and then a lot of variables. Can you tell us what that middle portion of the script is doing?

A. Yes. So the placement is, again, running a curl command against this Instance Metadata Service. That 169.254 IP address. And it's, again, asking information about the metadata, but specifically the availability zone portion of that metadata. So where that server is physically located and in which region.

The middle part of the code is checking if this placement or if this server is in U.S. east, then sets the mining pools in U.S. east or U.S. west servers that are related to Nanopool. Similar and so forth, if it's in the U.S. west or EU, essentially, it's assigning mining pools by Nanopool in a location that's closest to the current server.

Q. So the top lines, U.S. east, U.S. west, EU correspond to AWS Data Center regions?

A. Yes.

Q. And the rest corresponds to Nanopool regions?

A. Yes. The ones that reference Nanopool.org.

Q. Why would someone who's cryptomining want to have their Nanapool resources close to their AWS Data Center resources?

A. One is that you are within the same region as the server so that the traffic is going between -- you know, is not across the world, and it's staying locally, within a region, to evade

security or to evade being identified.

Secondly, it can also be good performance-wise because, as earlier testimony mentioned, that it is kind of like a competition to, you know, mine that block and report it. The closer you are to a pool that you can report that information to, the higher the performance it is, because, you know, instead of having to travel around the world to send that information, you're sending it to a server that's close.

MS. MANCA: Can we go to Exhibit 802?

Q. (By Ms. Manca) So this is minersetup_eth.sh. I'm going to talk to you and ask you to give us a high-level overview of how this script works.

A. Okay.

Q. Okay? What's the first thing it does?

A. So the first thing here is it's, you know, obtaining the repositories or resources to install certain applications onto that system.

Q. What do those applications do once they're installed?

A. It would depend on which application is being installed, but these are software repositories.

Q. Does the software perform any particular function?

A. I'm sorry? Are you asking about a specific one here or?

Q. Or just generally, what kind of software would she be downloading to use and for what purpose?

A. Yeah, there is a couple. You can see on kind of the first

lines, where it references Nvidia, or N-v-i-d-i-a. Nvidia is a company that's known to create graphic processing units, or GPUs. So this would contain, you know, software repositories to install applications that would allow the usage of that hardware.

Q. And then if we can pull out of this, there's just a bunch of numbers and letters that don't look like anything on the bottom half of this page. What's that?

A. So this is an encoding mechanism known as Base64 encoding. You'll see this throughout the script. You have a series of varying numbers and letters, and what Base64 encoding represents is data that is translated into this format. And what I mean by that is, you know, this type of representation for Base64 could represent the -- like a picture. So you can take a visual picture of what you are seeing, and then translate it to look like this.

There are many uses for this, particularly when you are having email communications; oftentimes, if you look at the email message behind the scenes, attachments and pictures are encoded in a similar way.

Q. So if you decode these aspects of this minersetup, what does it do?

A. So it depends, but in this one, it is a trusted private or public key that's being used to download additional software.

Q. And then we just looked at a docker file, a start "sh" with

those region pools and a wallet. How do those relate to this minersetup script?

A. They're also embedded in the script in a similar Base64 format.

Q. So if we were to decode these numbers and letters, we would get Exhibits 800 and 801?

A. Yes.

MS. MANCA: If we could pull up Exhibit 404, and then look at the very top quarter of that page.

Q. (By Ms. Manca) So this Slack message says, "For some reason, I lost a whole fleet of miners all at the same time. I think someone is on to me and they're using pool traffic info or something to correlate account miner IPS, so I'm gonna have to start using other wallet addresses." What's that mean?

A. The way I interpret this is that Ms. Thompson lost access to a wide number of cryptocurrency miners, and she believes that there's somebody that is, you know, identifying her miners and taking them down, so she's thinking about ways to change her tactics.

MS. MANCA: Can we do Exhibit 850? Actually, I don't think this is it. Can we unpublish?

Q. (By Ms. Manca) Do you recognize this print-up?

A. I do.

Q. How did you generate it?

A. This one was from the -- using the online blockchain

explorer ether_scan.

Q. And what does it show when you went to ether_scan?

A. This shows kind of the balance over time from the March time frame to the August time frame.

Q. Are these incoming transactions or account balance, or how -- why is the graph going up and down?

A. This would be the balance over time as it's going through the months.

Q. And what is the account that this relates to? Just the first, like, five.

A. Yeah. It's the 0x5a86 that's been referenced in the past and also within the cryptocurrency mining scripts.

MS. MANCA: Your Honor, we offer Exhibit 850.

THE COURT: 850 --

MR. KLEIN: No objection, Your Honor.

THE COURT: -- is admitted.

(Government Exhibit 850 admitted.)

MS. MANCA: May I publish?

THE COURT: Yes.

Q. (By Ms. Manca) And so can you recap your testimony now that we have the visual on the screen of the flow of the incoming transactions?

A. Yeah. So this is a graph of the Ether balance over the months. We can see there were a large number of Ether balances beginning in March, and then a slow decrease over the months.

MS. MANCA: Can we go back to Exhibit 802? And the last page of that exhibit. Can you highlight the bottom portion of that script?

Q. (By Ms. Manca) When you get to the very end of this script, what does that do?

A. Starting from docker run, that command will, essentially, create and run that docker instance onto the targeted system that it's on. So this would mean the deployment of a cryptocurrency miner. And then the last four commands are related to kind of hiding or deleting logs.

Q. What part of this script indicates that logs are being deleted?

A. Yeah. So if you look at the first -- or the last -- after the docker run section and the line after that, you see it's starting with, like, ln -sf, those two commands are removing or clearing out the bash history log.

The bash history log is what I mentioned earlier; the, kind of, history log of commands that were on a system. So the part where you type and when you press "enter," it gets recorded, those are being cleared.

The second part, where it says "find" space "/bar/log," what it's doing is going into this directory called "bar/log."

In a Linux file system, that is where, typically, most of the log files are stored when it's generated by applications, when it's generated by the operating system, or any type of

logging is usually stored in this directory, and what it's doing is clearing all of those out as well.

And then the final command RM, space, asterisk, "RM" stands for "remove," and asterisk is a keyword for "all." So what it's doing is also deleting every single file in its current directory.

Q. So whose logs are getting deleted?

A. The AWS EC2 instance that it's currently on.

Q. Is this script precise enough to delete logs that only relate to mining activity, or are all the logs being deleted?

A. So all the logs would be deleted in that directory.

Q. So if we can pull out of the code for a minute, and we'll just take the code off the screen, give our eyes a break, stretch, can you walk us through how this script is meant to be deployed?

A. Yes. So once Ms. Thompson has access to an AWS account, that is, again, the security credentials that allow it to authenticate in using the key, the secret access key and the token in that AWS environment using the AWS CLI to create new EC2 instance or servers using that run instance command.

Once these servers are created, other actions need to apply either before or after, but one of them would be to create an alternative way to access that newly created server. And in order to do that, depending on the environment for the victim, has a number of actions, one of them being creating a Secure

Shell or tunnel directly to that machine. In order to do that, she'd have to run AWS CLI commands, such as the one to create key pairs. So creating the key pairs sets that public key and that private key that allows an external user to authenticate into that computer.

However, there are certain environments where that type of remote connection, that SSH connection is not allowed. So there are times, too, where a security group has to be made, a new one. And a new security group would be made and also have a rule in it that would open a specific port. For SSH, this is port 22. So you would have a security group that creates port 22 and allows that to be open to anybody on the Internet, and you have a key pair that allows direct access to that Amazon EC2 instance, and three, it would have to have that role permission or that user account to create the server in the first place.

So once all those conditions are met, this would allow Ms. Thompson to connect directly to that machine now and transfer a file over, which, in this case, would be the minersetup_eth.sh, and then run that file onto that system in order to deploy the cryptocurrency miner.

MS. MANCA: Your Honor, can I offer Exhibit 122 for demonstrative purposes?

THE COURT: 122 is admitted for demonstrative purposes only and may also be displayed.

(Government Exhibit 122 admitted.)

MS. MANCA: And may I also use the blowup of that as well?

THE COURT: Sure.

Q. (By Ms. Manca) So, Mr. Ho, you just gave us a ton of information. We're going to unpack it.

Let's start on the left. There's something called SSH. What is SSH?

A. Yeah. SSH, again, stands for the Secure Shell. It is an application that allows you to create an encrypted tunnel or connection between two computers.

Q. What are the conditions that you need to create that tunnel between a virtual server instance and your own computer?

A. It will require an open port, by default SSH uses the port 22. And you'd also need a form of authentication, either a user name or a password or, in this case, a key pair.

Q. How do IAM Role credentials relate to creating the secured shell connection with key pairs and security groups?

A. So the IAM Role would be the credentials responsible for creating those things on an AWS environment. If that IAM Role has the permissions to do so, then it can create the ability to connect through SSH.

Q. So if I'm understanding what you said, the instance gets created, this new instance. Then you have the security groups and the key pairs that allow the secure connection between the new instance and Ms. Thompson's computer?

A. Yes.
Q. Okay. And then how does the script get deployed, this mine setup_eth?
A. There are multiple ways. One, you can copy the file using the AWS command line when you are creating that instance. Another is to connect directly to that computer and copy it over through SSH or through another type of Linux command.
Q. When this script is deployed, where in the instance is it designed to run?
A. It would be designed to run, typically, in the home directory of the newly created account, but it can be run anywhere.
Q. And is it downloaded to the computer, or does it run somewhere else?
A. It's downloaded onto that newly created EC2 instance, and then ran on the instance itself.
Q. What happens to the record of this script if an instance is terminated or taken offline?
A. So the way that this script is designed, it is running and launching the docker container in memory. And I've talked about memory before. It is a live piece of the device that is considered what's called volatile. So when the device is turned off, that volatile part, that RAM, is completely gone.
Since the script also deletes the logs and the files on the hard drive, both, in both cases, that evidence would be missing.

MS. MANCA: Can we pull up Exhibit 417, and then go down to page 2 and highlight that middle message at 79-2019. Yeah, that one.

Q. (By Ms. Manca) This says, "I changed the script to move everything and all of the work onto the RAM disk, which effectively leaves the customer unable to do any kind of forensic recovery."

How does that relate to what you've just testified about regarding active memory?

A. Yeah. So this explains what I just mentioned. It moves the cryptocurrency miner onto the RAM disk, which is another way to refer to the live memory.

MS. MANCA: And can we do Exhibit 414? And the middle part with some code and "CYA."

Q. (By Ms. Manca) In this Slack communication, Paige Adele says, "Aside from that one exception, I've got a pretty comprehensive CYA routine," and lists some code. What does that mean?

A. So CYA, that stands for covering yourself, your tracks, and making sure you're protected or safe from, you know, identification in this case.

And then the next part, where it's that type of information, and the context of this whole conversation is referring to a concept known as file system journaling, which is another way that forensic analysts can recover information about

what occurred on a system.

MS. MANCA: Can we go to Exhibit 670, page 2?

Q. (By Ms. Manca) So we've seen this script before -- it may seem like a million years ago -- but it's acquire AWS info?

A. Yes.

Q. Can you tell us which of the hash tags relate to cryptojacking or the conditions necessary for the installation of cryptocurrency miners?

A. I mean, a good majority can be used to aid in the assistance of accomplishing cryptojacking, but the key one here is towards the very end, lines 45 through 50, which is to attempt to create a key pair.

MS. MANCA: Can we go to Exhibit 456, page 2?

Q. (By Ms. Manca) This is a chat referring to a command RunInstances. It's got a reference to security groups, and then a limitation on the number of instances.

Can you tell us what the first two chats are referring to?

A. Yes. So the first part of the chat, you know, that command is used to create new servers. Just kind of quickly going through the command here, you see the region where it would have launched, which is in U.S. east; the instance type, you know, r5.large is a type of Amazon machine; count would mean how many servers of this type will you want to create, and this would be 100 servers; image ID is information about that Amazon image; and then to the security group is a very specific type of

security group identifier; and then all the additional things to create the server, with the last part with key name default, default is kind of the name of a key pair that we've seen in the previous script that was used to generate a new key pair.

And then the second line says -- it appears to be, you know, a response back from the Amazon command line, which says that, you know, the current environment that it's in, there's an instance limit or server limit. It says the quota for that account only allows 21 running instances, but the user had requested at least 100.

MS. MANCA: Thank you. And can we do Exhibit 456, page 4?

Q. (By Ms. Manca) Tell us what this means with the security group and the port 22.

A. Yeah. So this specific command authorize security group ingress is taking that security group that's listed there at the sg- and opening a port, specifically TCP port 22, which I mentioned before, is, you know, commonly used for SSH communication.

Q. On this drawing -- so we've got Exhibit 122, a physical blowup of it to your right. Where is port 22 on that drawing? It's not shown there, but where would it be?

A. It would be in several places, kind of, but really it would be at the EC2 part of that image there, that computer where the port is open.

But for the security group as well, it allows the ability to, you know, go through the other parts of -- it's going through the AWS environment or cloud. What I'm trying to say is there's -- you know, it's authorizing the computer to go directly to that EC2 instance at that port.

Q. We're talking about the AWS CLI. Where is the AWS CLI now?

A. Well, in this part, it's no longer needed, because the account, once SSH has been established, is an alternative way to get in or back-door way to get into this computer.

Q. Have you found evidence on Ms. Thompson's desktop computer that shows she was creating security groups and key pairs and Secure Shell connections?

A. Yes.

Q. What is that evidence?

A. So there's evidence of that in both the command line files, like the aws.commands file. There's evidence of that as well in the .sh folder that we've reviewed previously that showed --

MS. MANCA: Can we pull up 607 -- sorry. I didn't mean to cut you off.

Q. (By Ms. Manca) Is this the .ssh file you were just testifying about?

A. Yes.

Q. Can I show also you Exhibit 804? What is 804?

A. So this is the configuration or config file that's found within the .ssh folder within the Erratic user account on

Ms. Thompson's desktop computer.

And this file contains information about different hosts or computers to connect to, and it includes information about, for example, if it's an IP address or a domain to connect to. And there's sections here where you'll see where it says identity file. That would be the corresponding key that's used to authenticate.

Q. What, if any, conclusions can you draw from this file and the .ssh file and the other files you reviewed on the computer?

A. The conclusions I can draw is that there is evidence that indicates that Ms. Thompson's computer connected to these number of hosts. Certainly they were configured to connect to them with the existence of the keys, as well as entries in the known host's file in that folder, which, again, represents the log of computers that the desktop computer has connected to.

Looking at all of those tells me there is indicative of SSH connections going on to these hosts.

MS. MANCA: Can we show Exhibit 807?

Q. (By Ms. Manca) Do you recognize Exhibit 807?

A. Yes.

Q. What is that?

A. So this is a file called aws_scan.txt. This is also in the aws_hacking_shit folder.

Q. So we've been through a lot of steps this afternoon. What step are we looking at right now?

A. This is kind of going back to around, like, the second step, where there's information -- where Ms. Thompson is gathering information about the name of the IAM Roles that are associated with these IP addresses you see here on the left.

MS. MANCA: Can we go to the next page of the exhibit, please?

Q. (By Ms. Manca) And then what is happening here with this Waitrainer Role?

A. There, the aws_commands file, it appears that it was using those credentials and authenticating.

Q. Can we go to the next page? Is this from the config file?

A. It is, yes.

Q. And then we see a series of six data fields. What do those indicate?

A. Those indicate different host entries that are in the config file. So this provides information for the device when it's connecting to these hosts.

So, for example, if I say I want to connect to Waitrainer-1, it will know to connect to the IP address that's listed there and use the key that's listed there and use the user name that is listed there.

MS. MANCA: Can we go to the next page?

Q. (By Ms. Manca) This is a file IAM_fulllog.txt. What step in the process is this output?

A. This is still in that same step, kind of like the second

step, where you're obtaining information about the IAM Role.

MS. MANCA: Can we go to Exhibit 808, please?

Q. (By Ms. Manca) So this is a different IP address for a different user. Where is this AMI ID in the whole process we've just talked about?

A. This would be kind of around the first steps where you are just checking to see -- using your proxy scanner to see if you can even talk to the metadata service.

Q. And the next page, this is the second step?

A. Yes.

Q. Getting the IAM info?

A. Yes.

MS. MANCA: Can we go to the third page?

Q. (By Ms. Manca) This is from aws_commands. What kind of activity is happening in this data field?

A. So the first line is to --

MR. KLEIN: Your Honor, can we ask them to blow it up further?

THE COURT: Yeah, it's hard to read.

MR. KLEIN: We can't see anything.

MS. MANCA: Boy, I don't know that we can. The document cam might work. With these long txt files, it's difficult to zoom in, but we'll do our best.

THE COURT: That's better.

Q. (By Ms. Manca) So we'll start on this side and move slowly

over.

MS. MANCA: Agent, can you put it back? This is, again, going to be hard to read, but we're going to have do our best. Maybe just the first two-thirds.

Q. (By Ms. Manca) Okay. What's happening in this series of commands?

A. So in the first line, it's that curl command that you've seen before that is the getting the security credentials from the Instance Metadata Service and authenticating using that aws_session.sh script. The second line is to create a key pair. And the next two lines, the run instance lines, is creating servers, typically in the P3. family, which are high-compute servers under AWS, and is using the key pair that's generated along with -- you can see in the user data designation, that minersetup_eth.sh file.

The last two lines that include the authorized security group ingress indicate the security changes to open up port 22 to external users on the Internet.

Q. Let's go to Exhibit 809.

Which step is this, this megametadata.txt?

A. One of the beginning scripts, again, to identify that you can, at least, talk to the Instance Metadata Service.

Q. Okay. AMI ID is telling us we can talk to the Instance Metadata Service.

MS. MANCA: Can we go to the next page?

Q. (By Ms. Manca) And then this is the next step with a response?

A. Yeah. This is further obtaining the actual metadata information from the Instance Metadata Service as it relates to the IAM Role.

MS. MANCA: And can we go the next page? And the next page? Can you blow up the first half of that script?

Q. (By Ms. Manca) Can you just highlight a few of the commands that you see being run against this IP address?

A. So there's the first command that is authenticating against that IP address, but I see, you know, reconnoissance commands, the describe instances, describe security groups, those of that nature, but I also see create key pairs, as well as run instances to generate or create new servers.

THE COURT: Good place to stop?

MS. MANCA: Yes.

THE COURT: Okay.

All right. Long day, long week. Take a nice weekend off. Don't think about the case, don't do any research about the case, don't talk to anybody about the case.

Monday morning, remember, you don't need to be here till 10:20, and we'll get started at 10:30, so take your time Monday morning.

I would say we're on track to have the case to you by the end of next week. So we're slightly ahead of schedule, I would

say. So Thursday or Friday we'll do instructions and closing arguments. Now, we could slide a little bit, but that's where we're headed, I believe.

So have a great weekend, stay healthy, and we will see you Monday morning at 10:20. Leave your notepads on your chairs, and have a great weekend.

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: Please be seated. Did the government have anything before I boot you out?

MR. FRIEDMAN: I think we're slightly ahead of schedule, so I think we'll finish late Monday afternoon or possibly Tuesday morning, I would think by lunchtime.

And I think looking at our list, the one outstanding thing is the issue of the four Capital One's witnesses. I know Capital One's counsel is still here, and I know the court had talked about resolving that by the end of the day.

THE COURT: Well, I didn't say necessarily resolve by the end of the day. I said please keep talking to each other.

If we have a situation where somebody has COVID, of course we're not going to require them to come in. And if somebody is in Europe, we'll do it -- we'll work around the geographical and the time change and the health obstacles. But I can't make these guys commit any earlier than they need to.

So all I can tell you is we're not going to ask you to do

anything outrageous or unfair or unhealthy. Okay.

MR. PASTORE: Thank you, Your Honor. I think we're headed to virtual testimony.

THE COURT: That sounds like it to me, too.

MR. PASTORE: Thank you.

MR. HAMOUDI: May I? Before the government leaves, there's something I've got to put on the record that's related to this. This has to do with the subpoena that we issued to Amazon, and Mr. Buckley is here, he is a representative of Amazon.

The Court rejected an original subpoena that we issued, which was broad, early on. We issued a narrower one and they've not responded -- or they have. They do not want to give records, contracts. And based on testimony that we've heard, we're going to need more contracts, and then I'd like to make my proffer to the Court outside the presence of the government.

THE COURT: That's what you wanted to do outside the presence of the government?

MR. HAMOUDI: Yes.

THE COURT: So what can you tell me about what you're asking for with the government still here?

MR. HAMOUDI: I can tell you we're asking for contracts related to the victims alleged in Count 1, and then the 404 victims, which is the cryptomoney.

THE COURT: And the reason you need the contracts, is

that something you want to say outside the presence of the government?

MR. HAMOUDI: Yes.

THE COURT: Okay. All right.

So Mr. Buckley might have something he wants to say to me, too.

MR. HAMOUDI: That's why I introduced him, Your Honor; he may want to speak.

THE COURT: Mr. Buckley, would you like to address anything to me, or do it in writing?

MR. BUCKLEY: To the extent that -- first of all, Brian Buckley with Fenwick for Amazon.

To the extent we have anything to address with respect to the subpoena, I'll first have to hear the request and the argument before I know what I'm doing.

THE COURT: If I boot the government out, I'm booting everyone out.

MR. BUCKLEY: So do you want to hear our position on it without me knowing what they're going to argue to you?

THE COURT: Yes.

MR. BUCKLEY: May I come forward?

THE COURT: Yes, please come to the podium.

MR. BUCKLEY: So, Your Honor, I believe the request is for additional information about contracts between AWS and some of its customers for a larger period of time than AWS has

already produced.

So we have produced information about accounts with AWS customers that relate to the cryptojacking allegations or arguments.

THE COURT: Okay. That time frame.

MR. BUCKLEY: Right.

This, actually, came up before, when the defense filed a motion for an early response on their trial subpoena. You addressed these issues in your order, and I can get the docket number for you --

THE COURT: Oh, no. That's fine.

MR. BUCKLEY: -- and I said, I think, in fairly clear terms, that the broader range -- first, both the broader time range and the broader set of information wasn't relevant. And so I actually think you've already considered this and rejected it, but my understanding is they're renewing their request.

THE COURT: All right. Fair enough.

I'll ask everyone not part of the defense team to please leave and depart and have a great weekend.

Mr. Buckley, if you want to wait outside, we might be able to tell you something afterwards.

MR. BUCKLEY: Your Honor, can I clarify one thing?

THE COURT: Sure.

MR. BUCKLEY: The information that we've already produced is invoices that relate to the accounts, but not the

contracts themselves. So if I suggested otherwise, I wanted to correct that.

THE COURT: I appreciate that. Thank you.

(Courtroom is closed and the transcript is sealed.)

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

(Proceedings adjourned at 4:10 p.m.)

C E R T I F I C A T E

I, Nancy L. Bauer, CCR, RPR, Court Reporter for the United States District Court in the Western District of Washington at Seattle, do hereby certify that I was present in court during the foregoing matter and reported said proceedings stenographically.

I further certify that thereafter, I have caused said stenographic notes to be transcribed under my direction and that the foregoing pages are a true and accurate transcription to the best of my ability.

Dated this 10th day of June 2022.

/S/ Nancy L. Bauer

Nancy L. Bauer, CCR, RPR
Official Court Reporter